A REVIEW OF ACCESS CONTROL MEASURES AT OUR NATION'S AIRPORTS

HEARINGS

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION SECURITY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

FEBRUARY 3, 2015 and APRIL 30, 2015

Serial No. 114–1

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpo.gov/fdsys/

U.S. GOVERNMENT PUBLISHING OFFICE
94–105 PDF WASHINGTON : 2015

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

Michael T. McCaul, Texas, *Chairman*

Lamar Smith, Texas
Peter T. King, New York
Mike Rogers, Alabama
Candice S. Miller, Michigan, *Vice Chair*
Patrick Meehan, Pennsylvania*
Jeff Duncan, South Carolina
Tom Marino, Pennsylvania
Steven M. Palazzo, Mississippi**
Lou Barletta, Pennsylvania
Scott Perry, Pennsylvania
Curt Clawson, Florida
John Katko, New York
Will Hurd, Texas
Earl L. "Buddy" Carter, Georgia
Mark Walker, North Carolina
Barry Loudermilk, Georgia
Martha McSally, Arizona
John Ratcliffe, Texas

Bennie G. Thompson, Mississippi
Loretta Sanchez, California
Sheila Jackson Lee, Texas
James R. Langevin, Rhode Island
Brian Higgins, New York
Cedric L. Richmond, Louisiana
William R. Keating, Massachusetts
Donald M. Payne, Jr., New Jersey
Filemon Vela, Texas
Bonnie Watson Coleman, New Jersey
Kathleen M. Rice, New York
Norma J. Torres, California

Brendan P. Shields, *Staff Director*
Joan V. O'Hara, *General Counsel*
Michael S. Twinchek, *Chief Clerk*
I. Lanier Avant, *Minority Staff Director*

SUBCOMMITTEE ON TRANSPORTATION SECURITY

John Katko, New York, *Chairman*

Mike Rogers, Alabama
Earl L. "Buddy" Carter, Georgia
Mark Walker, North Carolina
John Ratcliffe, Texas
Michael T. McCaul, Texas *(ex officio)*

Kathleen M. Rice, New York
William R. Keating, Massachusetts
Donald M. Payne, Jr., New Jersey
Bennie G. Thompson, Mississippi *(ex officio)*

Amanda Parikh, *Subcommittee Staff Director*
Dennis Terry, *Subcommittee Clerk*
Vacancy, *Minority Subcommittee Staff Director*

* Honorable Patrick Meehan of Pennsylvania was elected to the committee effective April 14, 2015.

** Honorable Steven M. Palazzo of Mississippi resigned from the committee effective March 24, 2015.

CONTENTS

Page

TUESDAY, FEBRUARY 3, 2015

STATEMENTS

WITNESSES

PANEL I

PANEL II

FOR THE RECORD

THURSDAY, APRIL 30, 2015

STATEMENTS

WITNESSES

PANEL I

PANEL II

APPENDIX

A REVIEW OF ACCESS CONTROL MEASURES AT OUR NATION'S AIRPORTS

Tuesday, February 3, 2015

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON TRANSPORTATION SECURITY,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The subcommittee met, pursuant to call, at 2:33 p.m., in Room 311 Cannon House Office Building, Hon. John Katko [Chairman of the subcommittee] presiding.

Present: Representatives Katko, Rogers, Carter, Walker, Ratcliffe, McCaul, Rice, Payne, and Thompson.

Also present: Representative Johnson.

Mr. KATKO. The Committee on Homeland Security Subcommittee on Transportation Security will come to order.

The subcommittee is meeting today to hear testimony on the access control measures and employee vetting at airports around the country.

I now recognize myself for an opening statement. I would like to welcome everyone to the subcommittee's first hearing of the 114th Congress. I am honored to be the new Chairman of this important panel, which is charged with oversight of the Transportation Security Administration, commonly referred to as TSA. We are here about ensuring the security of our vast and vital transportation network as well.

Today's hearing on airport access control measures stems from a series of security breaches in which loaded weapons were brought onto commercial airplanes unbeknownst to TSA and airport officials. These alarming incidents could have had devastating consequences if those involved had intended to carry out the attacks.

The purpose of today's hearing is to examine current access control measures and employee vetting procedures and begin to identify short-term and long-term solutions to close any security loopholes. TSA spends billions of dollars every year to ensure every passenger is screened before boarding a commercial flight. That is an important responsibility. However, we must ask ourselves: What good is all the screening at the front door if we are not paying attention enough at the back door? The answer is common sense.

On December 23, 2014, for example, Federal agents arrested Eugene Harvey, a Delta baggage handler at Hartsfield-Jackson International Airport in Atlanta and charged him with trafficking in firearms and violating security agreements—requirements. Excuse me. Harvey allegedly work with a former Delta employee and used his security identification display area badge, commonly referred to as SIDA, to smuggle firearms, some of them loaded, onto passenger planes bound for JFK Airport in New York City.

The FBI called this a serious security breach and vowed to work to prevent future breaches. On January 13, Port Authority police in New York City arrested a Federal Aviation Administration official at LaGuardia Airport after he flew with a loaded firearm on a Delta flight from Atlanta to LaGuardia. The inspector, who flew inside the cockpit as part of his duties, had bypassed TSA screening in Atlanta by using his SIDA badge. The inspector was reassigned to other tasks, and the FAA has suspended its program that allows safety inspectors to bypass screening.

Finally, on January 24 of this year, the FBI arrested another Delta employee at Atlanta airport for boarding a flight to Paris without first being screened. He used his SIDA badge to gain entry to the sterile area of the airport. That investigation is on-going.

It raises concerns that all of the most recent breaches occurred at Atlanta, one of the world's busiest and largest airports. Having said that, though, these incidents are just some of the latest examples of breaches at our Nation's airports. These problems are not unique to just one airport. Every case presents unique challenges and opportunities for TSA, the airports, the airlines, and other partners to strengthen their security protocols. I am confident that we can improve background checks, training, security, and other measures, and I look forward to discussing these ideas today with our witnesses.

I also look forward to reviewing the recommendations of the Aviation Security Advisory Committee, otherwise known as ASAC, in roughly 90 days, following the ASAC's in-depth review of access control measures. Furthermore, I am planning to hold a follow-up hearing with my colleagues here focusing on that review, including how the ASAC's recommendations could be implemented at airports Nation-wide.

The reality is that the threats we face today are not the same threats we faced 2, 3, or even 4 years after 9/11. Nearly 14 years later, terrorists have adapted to our security protocols in ways that require us to be agile and resourceful. We cannot afford to be set in our ways and risk missing a glaring vulnerability. I hope this hearing is the beginning of a meaningful dialogue on the changes that need to be made at our Nation's airports.

[The statement of Chairman Katko follows:]

Statement of Chairman John Katko

February 3, 2015

I would like to welcome everyone to the subcommittee's first hearing of the 114th Congress. I am honored to be the new Chairman of this important panel, which is charged with oversight of the Transportation Security Administration (TSA) and ensuring the security of our vast and vital transportation network.

Today's hearing on airport access control measures stems from a series of security breaches in which loaded weapons were brought onto commercial airplanes unbeknownst to TSA and airport officials. These alarming incidents could have had devastating consequences if those involved had intended to carry out an attack.

The purpose of today's hearing is to examine current access control measures and employee vetting procedures, and begin to identify short-term and long-term solutions to close any security loopholes.

TSA spends billions of dollars every year to ensure every passenger is screened before boarding a commercial flight. That's an important responsibility. However, we must ask ourselves: What good is all of this screening at the front door if we are not paying enough attention to the back door? The answer is common sense.

On December 23, for example, Federal agents arrested Eugene Harvey, a Delta baggage handler at Hartsfield-Jackson Atlanta International Airport and charged him with trafficking in firearms and violating security requirements. Harvey allegedly worked with a former Delta employee and used his Security Identification Display Area (SIDA) badge to smuggle firearms, some of them loaded, onto passenger planes bound for JFK. The FBI called this a "serious security breach" and vowed to work to prevent future breaches.

On January 13, Port Authority police arrested a Federal Aviation Administration (FAA) Aviation Safety Inspector at LaGuardia airport after he flew with a loaded firearm on a Delta flight from Atlanta to LaGuardia. The inspector, who flew inside the cockpit as part of his duties, had bypassed TSA screening at Atlanta airport by using his SIDA badge. The inspector was reassigned to other tasks and the FAA has suspended its program that allows safety inspectors to bypass screening.

Finally, on January 24, the FBI arrested another Delta employee at Atlanta airport for boarding a flight to Paris without being screened. He used his SIDA badge to gain entry to the sterile area of the airport. The investigation is on-going.

It raises concern that all of the most recent breaches occurred at Atlanta, one of the world's largest and busiest airports. Having said that, these incidents are just some of the latest examples of breaches at our Nation's airports; these problems are not unique to just one airport. Every case presents unique challenges and opportunities for TSA, airports, airlines, and other partners to strengthen security protocols.

I am confident that we can improve background checks, training, screening, and other measures, and I look forward to discussing these ideas today with our witnesses. I also look forward to reviewing the recommendations of the Aviation Security Advisory Committee (ASAC) in roughly 90 days, following the ASAC's in-depth review of access control measures. Furthermore, I am planning to hold a follow-up hearing focusing on that review, including how the ASAC's recommendations could be implemented at airports Nation-wide.

The reality is that the threats we face today are not the same threats we faced 2, 3, or even 4 years after 9/11. Nearly 14 years later, terrorists have adapted to our security protocols in ways that require us to be agile and resourceful. We cannot afford to be set in our ways and risk missing a glaring vulnerability. I hope this hearing is the beginning of a meaningful dialogue on the changes that need to be made at our Nation's airports.

I now recognize the Ranking Member of the subcommittee, the gentlewoman from New York, Ms. Rice, for an opening statement.

Mr. KATKO. The Chairman now recognizes the Ranking Minority Member of the subcommittee, the gentlelady and former fellow prosecutor like me from New York, Miss Rice, for any statement she may have.

Miss RICE. Thank you, Mr. Chairman. Mr. Chairman, I ask unanimous consent that the gentleman from Georgia, Representative Hank Johnson, be allowed to sit and question the witnesses at today's hearing.

Mr. KATKO. Without objection, so ordered.

Miss RICE. Thank you, Mr. Chairman.

First, I want to thank you for convening this hearing. I want to express my eagerness to work with you and with all the Members of this subcommittee to do absolutely everything we can to maximize the security of our aviation sector.

The Transportation Security Administration's mission is to protect the Nation's transportation systems to ensure freedom of movement for people and commerce. The TSA stands on the front lines in the effort to protect the traveling public, but we know that they do not stand there alone. Aviation security is a truly collaborative effort.

Airports, vendors, airlines, and the TSA work as a team to prevent terrorists and criminals from harming the traveling public on the ground and in the air. All members of that team should be commended, as the aviation sector is stronger and more secure today than it has ever been. However, all members of that team must also be equally engaged in the effort to identify and correct any deficiencies in our aviation security. Recent incidents have revealed such deficiencies, vulnerabilities that exist within our airports, and must be swiftly addressed for the sake of our National security and for the safety of the American people.

Last December, authorities in my home State of New York uncovered a gun smuggling operation in which a former airline employee brought weapons and ammunition, 153 firearms, including an AK–47 assault rifle, aboard commercial flights in carry-on luggage over a period of several months before he was arrested selling weapons to undercover FBI agents on multiple occasions.

Also, in my home State just a few weeks ago, a safety inspector from the FAA was arrested at LaGuardia Airport after authorities discovered a firearm in his carry-on luggage. This individual flew from Atlanta to New York with a gun in his carry-on and was even allowed access to the cockpit, as the Chairman stated, while the plane was in the air.

It would be easy to point fingers at particular airports or airlines involved in these incidents, but that would overlook the most important lesson to be learned. Major deficiencies exist right now within our airport security systems. If these incidents can happen at one airport, they can happen at any airport. That is the reality we face, and we are here today to ensure that these deficiencies will be corrected as quickly and completely as possible.

What links these two incidents is that in both cases, the individuals exploited their SIDA credentials, their SIDA badges, to bypass security and bring prohibited items into secure areas. It is going to take a collaborative, comprehensive effort to ensure that on the front end SIDA badges are distributed only to individuals who have been thoroughly vetted and deemed worthy of being trusted with them and, secondly, to ensure that no one entrusted with a SIDA badge is exploiting it.

Again, I want to reiterate that this is and must always be a collaborative effort. It is my intent that, through open dialogue between all of the entities here today, we can successfully neutralize access control incidents and eliminate a major deficiency in our Nation's aviation security system.

I thank all of the witnesses for coming here before us today, and I yield back the balance of my time, Mr. Chairman.

[The statement of Ranking Member Rice follows:]

STATEMENT OF RANKING MEMBER KATHLEEN M. RICE

FEBRUARY 3, 2015

First, I want to thank you for convening this hearing, and I want to express my eagerness to work with you and with all the Members of this subcommittee to do absolutely everything we can to maximize the security of our aviation sector.

The Transportation Security Administration's mission is to "protect the Nation's transportation systems to ensure freedom of movement for people and commerce." The TSA stands on the front lines in the effort to protect the traveling public, but we know they don't stand there alone.

Aviation security is a truly collaborative effort. Airports, vendors, airlines, and the TSA work as a team to prevent terrorists and criminals from harming the traveling public on the ground and in the air. All members of that team should be commended, as the aviation sector is stronger and more secure today than it has ever been.

However, all members of that team must also be equally engaged in the effort to identify and correct any deficiencies in our aviation security. Recent incidents have revealed such deficiencies—vulnerabilities that exist within our airports and must be swiftly addressed for the sake of our National security and the safety of the American people.

Last December, authorities in my home State of New York uncovered a gun-smuggling operation in which a former airline employee brought weapons and ammunition—153 firearms, including an AK–47 assault rifle—aboard commercial flights in carry-on luggage over a period of several months, before he was arrested selling weapons to undercover Federal Bureau of Investigation agents on multiple occasions.

Also in my home State, just a few weeks ago, a safety inspector from the Federal Aviation Administration was arrested at LaGuardia Airport after authorities discovered a firearm in his carry-on luggage. This individual flew from Atlanta to New York with a gun in his carry-on, and was even allowed access to the cockpit while the plane was in the air.

It would be easy to point fingers at particular airports or airlines involved in these incidents. But that would overlook the most important lesson to be learned. Major deficiencies exist right now within our airport security systems, and if these incidents can happen at one airport, they can happen at any airport.

That is the reality we face, and we're here today to ensure that these deficiencies will be corrected as quickly and completely as possible.

What links these two incidents is that in both cases, the individuals exploited their Secure Identification Display Area credentials—also known as SIDA badges—to bypass security and bring prohibited items into secure areas.

It will take a collaborative, comprehensive effort to ensure that, on the front end, SIDA badges are distributed only to individuals who have been thoroughly vetted and deemed worthy of being trusted with them . . . And secondly, to ensure that no one entrusted with an SIDA badge is exploiting it.

I know that employee screening is a major component of the TSA's multi-layered strategy for addressing security vulnerabilities within the aviation sector. I look forward to hearing from Acting Deputy Administrator Hatfield today about how the TSA can further enhance this layer of security, and ensure that no unauthorized items make it into secure areas of airports.

I look forward to hearing from Mr. Southwell, the aviation general manager of Hartsfield-Jackson Atlanta International Airport, about the short, intermediate, and long-term solutions he plans to implement in order to reform his airport's security system and neutralize the insider threat.

Also with us today is Ms. Pinkerton, a member of the Aviation Security Advisory Committee, an entity that was codified into law through legislation offered by Ranking Member Thompson last Congress to advise on a wide variety of aviation security issues. As Ms. Pinkerton represents the perspective of multiple airports, I'm eager to hear her advice about what we can do across all our Nation's airports to eliminate this dangerous vulnerability.

Lastly, I look forward to Deputy Assistant Director Perdue shedding light on the FBI's involvement in incidents such as those I've mentioned, and to discuss the penalties associated with these breaches and whether those penalties are adequate and effective.

Again, I want to reiterate that this is and must always be a collaborative effort. It's my intent that through open dialogue between all of the entities here today, we can successfully neutralize access-control incidents and eliminate a major deficiency in our Nation's aviation security system.

Mr. KATKO. Thank you, Miss Rice.

The Chairman now recognizes the Chairman of the full committee, the gentleman from Texas, Mr. McCaul, for any statement he may have.

Mr. MCCAUL. I thank the Chairman.

I want to first congratulate you and Ranking Member Rice on your new position on this committee and by starting out this Congress with an important hearing that focuses on the importance of, and timely topic of, access control and employee screening at our Nation's airports.

It is vital that agencies responsible for protecting our airports are doing all that they can to keep safe our aviation sector. This responsibility does not end at the passenger screening checkpoints. A robust system, the vetting employees at airports is equally as important.

This hearing is an important opportunity to examine security programs designed to mitigate potential insider threats from airport employees, airline employees, TSA personnel, and others who have access to sterile areas of domestic airports.

In addition to the most recent access control breaches at Atlanta airport that have been mentioned, there have been a number of insider threats and employee issues at various other airports in recent years. For example, in December 2013, the FBI arrested an avionic technician at Wichita airport for plotting a suicide attack using a vehicle-borne improvised explosive device. The technician allegedly intended to use his airport clearance to gain access to the tarmac and detonate the vehicle near planes and the terminal during peak holiday travel in order to maximize casualties. He was charged with attempted use of a weapon of mass destruction and attempted to provide material assistance to al-Qaeda in the Arabian Peninsula.

Additionally, in September 2013, a TSA screener at Los Angeles International Airport was arrested a few hours after resigning his position for making threats against the airport that cited the anniversary of 9/11 and for leaving a suspicious package at the airport. His actions resulted in the evacuation of several airport terminals.

Finally, in September 2014, a former airline employee at Minneapolis airport died in Syria fighting alongside the Islamic State in Iraq and Syria. Though the individual had left employment with the airline several years prior to becoming a foreign fighter of ISIS, he did have access to areas of the airport during his employment, including the tarmac.

There are significant lessons to be drawn from these and other incidents involving employees. The bottom line is that our aviation network remains a prime target for terrorism. We must be vigilant and constantly reevaluate our security posture according to the threats that we face, and that includes potential insider threats.

I am pleased that this subcommittee will hear testimony from TSA and the FBI and airport and airlines representatives on this important topic, and I look forward to examining what additional measures should be taken to protect our airports and the American people.

With that, I yield back.

[The statement of Chairman McCaul follows:]

STATEMENT OF CHAIRMAN MICHAEL T. MCCAUL

FEBRUARY 3, 2015

I would like to commend Chairman Katko and Ranking Member Rice for starting off the Congress with focusing on the important and timely topic of access control and employee screening at our Nation's airports.

It is vital that the agencies responsible for protecting our airports are doing all that they can to keep our aviation sector safe. This responsibility does not end at the passenger screening checkpoints; a robust system of vetting employees at airports is equally as important.

This hearing is an important opportunity to examine security programs designed to mitigate potential insider threats from airport employees, airline employees, TSA personnel, and others who have access to sterile areas of domestic airports.

In addition to the most recent access control breaches at Atlanta airport that have been mentioned, there have been a number of insider threats and employee issues at various other airports in recent years.

For example, in December 2013, the FBI arrested an avionic technician at Wichita Airport for plotting a suicide attack using a vehicle-borne improvised explosive device. The technician allegedly intended to use his airport clearance to gain access to the tarmac and detonate the vehicle near planes and the terminal during peak holiday travel, in order to maximize casualties. He was charged with attempted use of a weapon of mass destruction and attempting to provide material assistance to al-Qaeda in the Arabian Peninsula.

Additionally, in September 2013, a TSA screener at Los Angeles International Airport was arrested a few hours after resigning his position for making threats against the airport that cited the anniversary of 9/11, and for leaving a suspicious package at the airport. His actions resulted in the evacuation of several airport terminals.

Finally, in September 2014, a former airline employee at Minneapolis Airport died in Syria fighting alongside the Islamic State in Iraq and Syria (ISIS). Though the individual had left employment with the airline several years prior to becoming a foreign fighter of ISIS, he did have access to sterile areas of the airport during his employment, including the tarmac.

There are significant lessons to be drawn from these and other incidents involving employees. The bottom line is that our aviation network remains a prime target for terrorism. We must be vigilant and constantly reevaluate our security posture according to the threats we face, and that includes potential insider threats.

I am pleased that the subcommittee will hear testimony from TSA, the FBI, and airport and airline representatives on this important topic and I look forward to examining what additional measures should be taken to protect our airports and the American people.

I thank Chairman Katko for his leadership of the subcommittee and I yield back the balance of my time.

Mr. KATKO. Thank you, Mr. Chairman.

The Chairman now recognizes the Ranking Minority Member of the full committee, the gentleman from Mississippi, Mr. Thompson, for any statement he may have.

Mr. THOMPSON. I thank the Chairman for holding today's hearing. I also welcome both you and the Ranking Member of this committee.

After the horrific attacks of September 11, 2001, multiple layers of security were put in place to protect our aviation system. Not only did screening procedures and the list of prohibited items change, but the protocols for security of the airports changed as well.

While Congress and Executive branch were making considerations to keep the traveling public safe, they also recognized that there are 450 airports in the United States, each of which presents a unique set of security issues. For instance, vendors and airline employees need access to various areas of the airport. In an effort to maintain security and provide a sense of practicality to airport and airline employees, legislation was implemented to allow vetted individuals to have unescorted access within the areas that lie beyond airport secure screening checkpoints.

Airline and airport employees are vetted through a criminal background check and biographical check. They are issued Secure Identification Display Area badges, commonly referred to as SIDA badges, to use to gain access to a sterile area of the airport without having to go through physical screening.

While SIDA badge holders are vetted daily against a terrorist watch list, the criminal background checks are not conducted recurrently. Mr. Chairman, this is concerning. In 2011, the Office of Inspector General found that some of the records provided by employees contain inaccuracies or omissions and that TSA had limited oversight of the application process.

Moreover, recent events have me questioning whether TSA has taken seriously the recommendations of the OIG. I still question whether airports and TSA have the adequate internal controls to address potential insider threats from SIDA badge holders. Do employees retain badges upon termination? Are logs kept on the number of lost or stolen badges? Are badges being used to gain access only when an employee is on duty?

Unfortunately, in December 2014, we saw a deplorable instance of SIDA badge misuse. Five men were charged in connection with a plot to smuggle over 150 guns from Atlanta to New York City. One of these men is alleged to have used his credentials to get by physical screening and board flights to New York City. Although the weapons were not intended to harm passengers, and these men have not been charged with terrorism, it is disheartening to think of a catastrophic consequence that could have occurred had one of those firearms been used on the airplane during the flight.

Mr. Chairman, as you know, the threat is evolving. As it evolves, we cannot remain stagnant. It is my hope that through our continued oversight and bipartisan legislative work, we can make sure there are proper policies and procedures in place to ensure that those that have access to a sterile area of the airport cannot create such gross breaches of security. The security of an airport is a shared concern, and all entities should work together to ensure that the layers of security are as strong as they can be.

With that, Mr. Chairman, I look forward to today's testimony. I yield back.

[The statement of Ranking Member Thompson follows:]

Statement of Ranking Member Bennie G. Thompson

February 3, 2015

After the horrific attacks of September 11, 2001, multiple layers of security were put in place to protect our aviation system. Not only did screening procedures and the list of prohibited items change, but the protocols for security of the airports changed as well. While Congress and the Executive branch were making considerations to keep the traveling public safe, they also recognized there are 450 airports in the United States, each of which presents a unique set of security issues.

For instance, vendors and airline employees need access to various areas of the airport. In an effort to maintain security and provide a sense of practicality to airport and airline employees, legislation was implemented to allow vetted individuals to have unescorted access within the areas that lie beyond airports' secure screening checkpoints. Airline and airport employees are vetted through a criminal background check and biographical check. Then they are issued Secure Identification Display Area (SIDA) Badges to use to gain access to the sterile area of the airport without having to go through physical screening. While SIDA badge holders are vetted daily against the terrorist watch lists, the criminal background checks are not conducted recurrently.

Mr. Chairman, this is concerning. In 2011, the Office of Inspector General found that some of the records provided by employees contained inaccuracies or omissions and that TSA had limited oversight of the application process. Moreover, recent events have me questioning whether TSA has taken the recommendations of the OIG seriously. I still question whether the airports and TSA have the adequate internal controls to address potential insider threats from SIDA badge holders. Do employees return badges upon termination? Are logs kept on the number of lost or stolen badges? Are badges being used to gain access only when an employee is on duty?

Unfortunately, in December 2014, we saw a deplorable instance of SIDA badge misuse. Five men were charged in connection with a plot to smuggle over 150 guns from Atlanta to New York City. One of these men is alleged to have used his credentials to get bypass physical screening and board flights to New York City.

Although the weapons were not intended to harm passengers, and these men have not been charged with terrorism, it is disheartening to think of the catastrophic consequences that could have occurred had one of those firearms been used on the airplane during the flight.

Mr. Chairman, as you know, the threat is evolving. As it evolves, we cannot remain stagnant. It is my hope that through our continued oversight and bipartisan legislative work, we can make sure there are proper policies and procedures in place to ensure that those that have access to the sterile area of the airport cannot create such gross breaches of security. The security of an airport is a shared concern, and all entities should work together to ensure that the layers of security are as strong as can be.

Mr. KATKO. Thank you, Mr. Thompson.

Other Members of the committee are reminded that opening statements may be submitted for the record.

Now, we are pleased to have several distinguished witnesses before us today on this important topic. Let me remind the witnesses that their entire written statements will appear in the record.

Our first witness, Mr. Hatfield, is the acting deputy administrator at the TSA. Prior to his current role, Mr. Hatfield served as a Federal security director for Newark Liberty International Airport, where he managed a security force over 1,200 employees. He has been with TSA since 2002, has held a number of roles including assistant administrator of strategic communications and public affairs.

The Chairman now recognizes Mr. Hatfield to testify.

STATEMENT OF MARK HATFIELD, ACTING DEPUTY ADMINISTRATOR, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. HATFIELD. Thank you very much, sir.

Good afternoon, Chairman Katko, Ranking Member Rice, distinguished Members of the committee.

Chairman McCaul and Mr. Thompson, it is great to see you all here as well. I am personally honored and thrilled for the opportunity to have this conversation with you.

After I finish with the requisite reading of my prepared statement, I am really looking forward to an energetic conversation, and I hope that I can provide enlightening answers to your questions.

As you know, last December an investigation revealed that a Delta Airlines employee allegedly conspired to smuggle firearms from Hartsfield-Jackson International Airport to John F. Kennedy International Airport in New York, and a Federal prosecution is now under way in this case. While I am currently unable to comment in any detail on the specifics of these allegations, I can assure you that TSA views with great concern and focus any potential instance of security vulnerabilities. We are fully engaged with our aviation industry partners, and we look at all options to ensure the continued security of our Nation's commercial aviation and other transportation networks.

In addition to coordinating efforts with industry stakeholders, we are also working closely with our colleagues at the Department of

Homeland Security. In fact, Secretary Johnson personally visited Atlanta to speak with our partners at that airport. I can report to you that TSA has taken immediate steps to increase mitigation efforts of the insider threat. These steps include increasing operations that focus on screening airport employees at employee entrances and direct access points, such as secure doors and elevators and vehicle gates. In partnership with airport authorities, TSA is further examining circulation controls and reassessing employee access points, both the number and design of those access points.

Many of our Nation's airports are open for business around the clock, and numerous entities support air travel by providing amenities such as food and shopping throughout the airport. While the sterile area of an airport hosts passengers and aircrews waiting for flights, it is also the workplace and break space for vendors, mechanics, ground crew, and others.

Enforcing access control is a shared responsibility among multiple partners. I appreciate your pointing that out in your opening statement, Madam Rice. Every airport and airline has a security plan that reflects this. Airport authorities and the airlines are responsible for developing and executing these security plans. TSA is responsible for approving them and using our authority to perform inspections for compliance and comportment with those rules. Each airport operator must allow TSA at any time or place to make any inspection or test to determine compliance with TSA's regulations and other policies.

TSA is currently conducting an insider threat analysis to help better identify indicators of criminal acts or threats to aviation. This is the type of critical thinking we use to improve training, operations, and methods of screening. Additionally, TSA Acting Administrator Carraway has asked the Aviation Security Advisory Committee, the ASAC, to specifically review access control and perimeter security issues and offer their recommendations to address potential threats. I, in fact, met with them yesterday. I met with the larger body and their Chairman, and they are meeting again today. We are eager to see their recommendations. They are reporting at 30-, 60-, and 90-day threshold marks. That first report is due at the end of this week. Mr. Chairman, thank you for recognizing the work that they are doing.

TSA also conducts security background checks for airport and airline employees. Airport workers are vetted before they are granted unescorted access to the secure areas of the airport, and TSA performs a security threat assessment on all airport workers who require a credential. Once TSA has completed the check, information is provided to the individual's prospective employer with access either granted or denied based on the results of the security threat assessment.

We also continuously check all SIDA holders against the terrorist screening center's database to see if there are any changes in their status. That is an on-going, daily, continual check against that dynamic list.

In Atlanta and in airports across the country, TSA performs physical screening of employees with SIDA badges and sterile area access to entrances of these areas of the airport, places like bus stops for employees, employee turnstiles, and airport entry gates.

Following the revelation of the alleged smuggling operation in Atlanta, it has been suggested by some that airports institute 100 percent screening of all employees any time they enter or re-enter a secure area. In 2008, TSA actually conducted pilot programs comparing the screening effectiveness of 100 percent airport employee screening versus a program that includes continuous random and unpredictable employee screening measures.

In that same year, the Homeland Security Institute, HSI, independently assessed those pilot programs and concluded that 100 percent physical screening of all airport employees is both cost-prohibitive and poses a wide range of operational challenges without delivering demonstrably greater security. In other words, HSI also determined that random screening, properly done, is nearly as effective as 100 percent screening.

As a result of the TSA pilot and the HSI report, TSA made recommendations to enhance access control security. They include: The order to accelerate the installation of closed-circuit television and perimeter intrusion detection systems, phasing in the use of biometric access controls and identity verification systems, increasing security awareness training for airport workers, and increasing the Visible Intermodal Prevention and Response teams known as our VIPR teams operations.

Having recently served as TSA's Federal security director in Miami, an airport that does conduct 100 percent employee screening, I can tell you without question that such a practice involves both a significant investment of resources and is operationally challenging. That said, I have great respect for my former partners in Miami and the extraordinary commitment that they make as an airport, sometimes unilaterally, and without the force of a Federal regulation or rule to continually look at ways to make that airport safer.

TSA has an important role, in partnership with airport operators and airlines, in securing access to our Nation's airports, and we are committed to risk-based security solutions that enhance our current posture.

I want to thank the committee for the opportunity to testify today, and I do look forward to your questions. Thank you.

[The prepared statement of Mr. Hatfield follows:]

Prepared Statement of Mark Hatfield

February 3, 2015

Good afternoon Chairman Katko, Ranking Member Rice, and distinguished Members of the committee. I appreciate the opportunity to appear before you today to discuss the Transportation Security Administration's (TSA) role in airport access control at our Nation's airports.

The primary mission of TSA is to reduce security vulnerabilities and to strengthen resilience against terrorist attacks in the Nation's transportation systems, including aviation, mass transit, rail, highway, and pipeline, to ensure freedom of movement for people and commerce. To fulfill this vital mission, TSA employs a risk-based, layered approach to security through a well-trained front-line workforce, state-of-the-art technologies, intelligence analysis and information sharing, explosives detection canine teams, Visible Intermodal Prevention and Response teams, and our industry partners who voluntarily adopt security improvements and comply with regulations. This multi-layered approach helps to ensure that resources are applied efficiently to have the greatest impact in reducing risk and enhancing the security of the traveling public and the Nation's transportation systems.

ACCESS CONTROL

Each day, TSA facilitates and secures the travel of nearly 2 million air passengers at nearly 450 airports Nation-wide. Numerous entities are involved in supporting safe and secure travel as well as providing amenities such as food, shopping, and other entertainment. Controlling access to sterile, (post-security screening checkpoint) airport areas is a critical part of airport operations. While the sterile area hosts passengers and air crews waiting for flights, it is also the workplace for vendors, mechanics, ground crew, and others employed by the airlines and the airports. Access control is a shared responsibility among many partners, and every airport and airline has a security plan of which access control is an important and necessary element. Airport authorities and the airlines are responsible for developing and executing security plans; TSA is responsible for approving security plans and inspecting for compliance.

TSA's inspections include credentialing, perimeter security, and testing of access control systems and processes at airports. Every commercial airport receives an annual security inspection to include an assessment of perimeter and access controls. TSA analyzes the results of these inspections and assessments to develop mitigation strategies to enhance airport security.

Transportation Security Officers and Inspectors are also deployed on a random and unpredictable basis to screen airport and airline workers as they enter for work within the secure and sterile areas. The screening protocols vary by time, location, and method to enhance unpredictability. This includes ID verifications, and searches of individuals and/or their property, using various technologies and methods in order to detect and deter the introduction of prohibited items. Additionally, airport operators are required to conduct random inspections of employees entering sterile areas, to include ID verification and checks for prohibited items. If employees fail to follow proper procedures in accessing secure areas, they may be restricted from future access, disciplined by their employer, or subject to criminal charges and civil penalties.

TSA has wide-ranging authority to pursue inspections of airport security plans. Each airport operator is required to allow TSA, at any time or place, to make any inspections or tests, to determine compliance of an airport operator, aircraft operator, foreign air carrier, indirect air carrier, or other airport tenants with TSA's regulations, security programs, security directives, and other policies. Inspections and audits are conducted by our Compliance Division and, in situations of possible non-compliance, investigations are undertaken by Transportation Security Inspectors. Enforcement Investigation Reports that yield evidence of non-compliance are jointly overseen by the airport's Federal Security Director and by the Office of Security Operation's Compliance Division.

VETTING AND BADGING PROCESS

In addition to our regulatory role, TSA also conducts security background checks for airport and airline employees through the Secure Identification Display Area (SIDA) badging process. Airport workers are vetted before they are granted unescorted access to the secure area of the airport. TSA performs a Security Threat Assessment (STA) on those who require access to the secure/sterile area of the airport or unescorted access to cargo. When individuals apply for employment with the airport or airline, they submit STA information which is passed through one of several vendors to TSA for adjudication. This includes a check against the Terrorist Screening Database (TSDB). In partnership with the FBI and Customs and Border Protection (CBP), the individual also undergoes a Criminal History Background Check and immigration status check. Once TSA has completed the check, the information is provided to the individual's prospective employer with access either granted or denied based on the results of the STA. TSA also continuously checks all SIDA holders against the TSDB in case there are any changes to their status.

With TSA's Risk-Based Security model, similar to what we do with trusted travelers in TSA Pre✔™ or Known Crew Member, airport workers are vetted before they are granted unescorted access to the secure area of the airport. With the STA, we weed out potential bad actors, which is particularly important given the sensitive areas where many of these individuals work. However, we must balance the importance of conducting checks on employees with the need to facilitate air travel, and so have designed a system of background checks, inspections, and random checks as a risk-based approach to access control.

STUDIES AND RECOMMENDATIONS

In 2011, the Office of Inspector General (OIG) assessed TSA's efforts to identify and track access control at airports, specifically whether TSA had an effective mechanism to identify measures that could be used to improve security Nation-wide. The OIG found that without an effective mechanism to gather information about all security breaches, TSA was unable to monitor trends or make general improvements to security. The OIG made recommendations to use one comprehensive definition of a security breach as well as to develop a comprehensive program to ensure accurate reporting and corrective actions in breach incidents. As a result, TSA developed a single definition of "Security Breach," and enhanced its oversight system with respect to airport security breaches. TSA now leverages the Performance and Results Information System (PARIS) to accurately report, track, and analyze access control trends. Further, TSA updated airport performance metrics to track security breaches and airport checkpoint closures at the National, regional, and local levels.

In 2008, TSA conducted a study to compare two approaches to physically screening airport employees: Screening 100 percent of airport employees or conducting random screening measures. Three airports tested the 100 percent screening model and another four screened employees on a random basis. The Homeland Security Institute (HSI) independently assessed the pilot programs using three factors: Screening effectiveness, effect on airport operations, and cost considerations. HSI concluded that 100 percent physical screening of all airport employees is cost-prohibitive and poses a wide range of operational challenges. For instance, many employees wear steel-toed shoes for safety at work; however this poses a unique challenge and delay in screening through a magnetometer. Additionally, airports conducting 100 percent screening reported delays, ranging from minor at smaller airports to major at larger ones.

HSI also determined that random is nearly as effective as 100% screening, stating that they "did not see a clear distinction between the number of items confiscated at 100% versus random screening airports." Given the HSI and TSA pilot results, TSA made the following recommendations for airports to enhance access control security:

- Accelerate the installation of closed-circuit television and perimeter intrusion detection systems;
- Raise physical screening levels for airport employees (TSA and airport operators);
- Phase in the use of biometric access controls and identity verification systems;
- Focus on locally-driven security solutions (Community Policing and Airport Watch);
- Increase security awareness training for airport workers;
- Increase Visible Intermodal Prevention and Response teams and surge operations (random and threat-based); and
- Promote behavior-based threat detection programs.

In 2009, the Government Accountability Office (GAO) addressed the issue of insider threats in a review of TSA's efforts to secure commercial airport perimeters and access controls. Using data from the 2008 tests referenced above, GAO reported that physically screening 100 percent of employees would range from $5.7 billion to $14.9 billion for the first year, while the costs of enhancing random worker screening would range from $1.8 billion to $6.6 billion. This audit, entitled *A National Strategy and Other Actions Would Strengthen TSA's Efforts to Secure Commercial Airport Perimeters and Access Controls*, provided five recommendations to further TSA's efforts to enhance the security of the Nation's airports through a unifying National strategy that identifies key elements, such as goals, priorities, performance measures, and required resources. TSA concurred with and implemented the recommendations of this audit.

INSIDER THREAT MITIGATION

In December 2014, an investigation revealed that a Delta airlines employee allegedly conspired to smuggle firearms from Hartsfield-Jackson Atlanta International Airport (ATL) to John F. Kennedy International Airport (JFK) in New York, and a Federal prosecution is under way in this case.

To reduce risks exposed by this criminal conspiracy, TSA has implemented a variety of measures and is examining how this case can inform airport security more broadly. As described above, TSA administers Security Threat Assessments for all airport and airline employees prior to the issuance of SIDA badges granting unescorted access privileges. TSA also vets these individuals on a recurring basis against the Terrorist Screening Database. At ATL and Nation-wide, TSA requires the airport authority to randomly perform physical screening of employees with

SIDA badges at a variety of unpredictable locations such as Secure Area access points, employee bus stops, employee turnstiles, and airport entry gates. In calendar year 2014, TSA performed 7,234 hours of such screening at ATL and 257,979 hours Nationally.

TSA has taken immediate steps at ATL to mitigate the insider threat. Under the leadership of TSA officials, a working group was created with representation from various airport authorities, law enforcement, and stakeholders to further develop plans for improving security. TSA has increased operations to focus on screening airport employees at employee entrances and direct access points, such as turnstiles, Secure Area doors and elevators, and vehicle gates. Air carriers at ATL have also implemented additional security measures to address the issue. In partnership with airport authorities, TSA is further examining circulation controls and reassessing employee access points. We look forward to a continued partnership with key stakeholders to determine best practices and risk-based security solutions that could be replicated in other airports.

On a broader level, TSA is examining the potential vulnerabilities exposed by this incident and other trends to determine if additional risk-based security measures, resource reallocations, new investments, or policy changes may be necessary. TSA is conducting an insider threat analysis to identify potential indicators of criminality or threats to aviation that could provide insight into new training, operations, or methods of screening and vetting employees. TSA is examining its legal authorities to assess if additional measures may be required or imposed to enhance security. Finally, TSA Acting Administrator Carraway has asked the Aviation Security Advisory Committee (ASAC) to specifically review access control and perimeter security issues to offer solutions to potential threats.

CONCLUSION

TSA plays an important role in partnership with airports and airlines in securing access to our Nation's airports, and is committed to fielding responsive, risk-based solutions that can enhance our current security posture. I want to thank the committee for your interest in this important issue and your support as we consider recommendations and future changes to improve aviation and airport security Nationwide. Thank you for the opportunity to testify today, I look forward to your questions.

Mr. KATKO. Thank you, Mr. Hatfield, for your testimony. We appreciate you being here today. I appreciate and I look forward to the dialogue that is forthcoming.

Our second witness is Mr. Gary Perdue, who currently serves as deputy administrative director of the counterterrorism division at the FBI. Mr. Perdue has over 30 years of U.S. Federal Government service—he beats me—specializing in military intelligence, foreign counterintelligence, drug trafficking, international terrorism, weapons of mass destruction, and counterproliferation. Prior to his current position, Mr. Perdue was the special agent in charge of the FBI's Pittsburgh division.

The Chairman now recognizes Mr. Perdue to testify. Thank you, sir.

STATEMENT OF G. DOUG PERDUE, DEPUTY ASSISTANT DIRECTOR, COUNTERTERRORISM DIVISION, FEDERAL BUREAU OF INVESTIGATION, U.S. DEPARTMENT OF JUSTICE

Mr. PERDUE. Thank you. Good afternoon, Chairman Katko, Ranking Member Rice, and Members of the subcommittee.

Thank you for the opportunity to appear before you today and for your continued support of the men and women of the Federal Bureau of Investigation.

I am particularly pleased to be here today with Mark Hatfield, the acting deputy administrator of the Transportation Security Administration, to discuss our role in access control measures at our Nation's airports.

Today's FBI is a threat-focused, intelligence-driven organization. Every professional understands—excuse me—every FBI professional understands that preventing the key threats facing our Nation means constantly striving to be more efficient and more effective.

Just as our adversaries continue to evolve, so too must the FBI. We live in a time of acute and persistent terrorist and criminal threats to our National security, our economy, and to our communities. These diverse threats illustrate the complexity and breadth of the FBI's mission, and make clear the importance of its partnerships, especially with the TSA, in reducing security vulnerabilities in our Nation's transportation system.

In fact, our National headquarters and local field offices have built partnerships with just about every Federal, State, local, Tribal, and territorial law enforcement agency in the Nation. Our agents, analysts, and professional staff work closely with law enforcement, intelligence, and security services to include representatives at our Nation's airports and airlines to mitigate the threat posed to our Nation's transportation infrastructure and internal aviation security processes and systems. By combining our resources and leveraging our collective expertise, we are able to investigate National security threats that cross both geographical and jurisdictional boundaries.

Our civil aviation security program: In conjunction with our partners, the FBI's counterterrorism division's Civil Aviation Security Program, also known as CASP, is extensively involved in efforts to undercover and prevent terrorist operations to attack or exploit civil aviation in the United States. The FBI has special agents and task force officers assigned as airport liaison agents at each of the Nation's TSA-regulated airports in order to respond to aviation-related incidents and threats, participate in joint FBI-TSA airport vulnerability assessments, and interact with interagency and private-sector stakeholders at airports around the country on exercises, threat mitigation, and other issues to protect the traveling public.

The FBI's CASP and ALA program were created in 1990 to formalize the Bureau's investigative intelligence and liaison activities at the Nation's airports. CASP is located in the FBI's National Joint Terrorism Task Force, with a focus on supporting and enhancing efforts to prevent, disrupt, and defeat acts of terrorism directed toward civil aviation and to provide counterterrorism preparedness leadership and assistance to Federal, State, and local agencies responsible for civil aviation security.

One of CASP's primary responsibilities is to provide program management and support to the FBI's airport liaison agencies. In addition, CASP represents the FBI on aviation security policy matters, provides guidance and training to the field, and supports National aviation security initiatives and mandates.

I would like to go over briefly CASP efforts to mitigate the insider threat at America's airports. Our intelligence production. Since 2009, CASP has produced numerous intelligence products that are shared with the U.S. intelligence community. A couple of the Unclassified products titles include: "Aviation-related Suspicious Activities: An FBI Assessment" on 3 June 2005. "Terrorist

Training Document Reveals Travel Guidance and Tactics" on 13 October 2009.

To further mitigate threats to aviation, CASP produces and distributes a comprehensive daily aviation-centric intelligence summary for all airport liaison agents and various FBI programs. This summary includes the latest threats to: Aviation, suspicious activity reporting within the air domain, current intelligence reporting, and updates on active aviation cases of importance.

In addition, CASP intelligence analysts produce threat intelligence reports yearly in support of Congressionally-mandated FBI-TSA joint airport vulnerability assessments, also known as JAVAs, and coordinate on-sight preparation, representation at JAVA events.

Our liaison: CASP has conducted three FBI air carrier security director forums since 2011, with a 3-day forum planned for August of this year. CASP has published nine aviation-centric Operation Tripwires since 2003, with a 2010 Operation Tripwire that addressed the insider threats specifically. For those of you not familiar with the FBI's Operation Tripwire, it began in 2003 as a counterterrorism division initiative designed to improve the FBI's intelligence and information base.

The program's vision is to develop FBI partnerships that help to identify U.S.-based terrorist sleeper cells through collecting and assessing specific information related to potential counterterrorism threats. The program's goal is to leverage outreach programs focused on aiding industry and local officials in recognizing suspicious activity and providing them a point of contact for reporting that activity, as well as to provide actionable items for the Joint Terrorism Task Force. CASP proactively develops curriculum on aviation security issues and providing training to ALAs, other Government agencies, the private sector, and foreign governments.

Our operational support: CASP provides operational support to the FBI's ALAs and substantive units on active investigations and provides strategic intelligence products on terrorist tactics, techniques, and procedures. CASP responds to official requests for information request for assistance, requests related to investigations of laser pointer illuminations of aircraft, unmanned aerial vehicle incidents, Government Accountability Office inquiries, National Transportation Safety Board aircraft accident investigation assistance, aviation-related exercises, and hijacking response plans involving ALA and FBI equities.

CASP developed a series of ALA best practices that leverages division-specific initiatives for broad participation by all FBI divisions and ALAs. These initiatives include: Documents and guidance on conducting vulnerability assessments at general aviation airports under the general aviation assessments initiative, issuing Federal misdemeanors for non-felonious criminal acts at airports under the Federal misdemeanor violations best practice, conducting recurring criminal record checks through the FBI's National Crime Information Center on airport employee under the air domain computer information comparison initiative, and providing checklist and guidance for handling a major aviation crisis such as a commercial airline crash under the aviation crisis response checklist best practice initiative.

CASP also has access to the Federal Aviation Administration-managed domestic events network, allowing for enhanced response and situational awareness during real-time aviation incidents.

Our training: One of CASP's major focus areas is conducting training for the FBI's ALAs, other Government agencies, and private-sector stakeholders. CASP has led the way with innovative cost-saving training initiatives that include: A 2011 CASP-conducted joint FBI-NTSB-ALA regional training, instructing attendees on how to handle issues surrounding a major aviation crisis within their area of responsibility, conducted three FBI ACSD forums since 2011. CASP launched a mandatory ALA-specific virtual academy training course for FBI employees entitled Airport Liaison Agent Fundamentals in 2012.

CASP recently worked with ALA coordinators for in-depth training at Los Angeles International Airport, Los Angeles, California on 10 through 11 September 2014. CASP represents the FBI's equities on various interagency and industry committees working groups such as: The Air Domain Awareness Working Group, Man Portable Air Defense Systems Analysis Working Group, Secondary Barrier Working Group, Civil Aviation Threat Working Group, Aviation Information-Sharing Working Group, the Air Domain Intelligence Integration and Analysis Center Working Group, Unmanned Aircraft Systems Event Reporting Working Group, and International General Aviations Working Group.

In conclusion, Chairman Katko, Ranking Member Rice, thank you again for this opportunity to testify concerning access control measures at our Nation's airports. The FBI's efforts and successes would not be possible without the continued positive working relationship with our partners and with your support. I would be happy to answer any questions that you might have. Thank you.

[The prepared statement of Mr. Perdue follows:]

Prepared Statement of G. Doug Perdue

February 3, 2015

INTRODUCTION

Good afternoon Chairman Katko, Ranking Member Rice, and Members of the subcommittee. Thank you for the opportunity to appear before you today and for your continued support of the men and women of the Federal Bureau of Investigation (FBI). I am particularly pleased to be here today with Mark Hatfield, the acting deputy administrator of the Transportation Security Administration (TSA) to discuss our role in access control measures at our Nation's airports.

Today's FBI is a threat-focused, intelligence-driven organization. Every FBI professional understands that preventing the key threats facing our Nation means constantly striving to be more efficient and more effective.

Just as our adversaries continue to evolve, so, too, must the FBI. We live in a time of acute and persistent terrorist and criminal threats to our National security, our economy, and to our communities. These diverse threats illustrate the complexity and breadth of the FBI's mission and make clear the importance of its partnerships, especially with the Transportation Security Administration, in reducing security vulnerabilities in our Nation's transportation system.

In fact, our National headquarters and local field offices have built partnerships with just about every Federal, State, local, Tribal, and territorial law enforcement agency in the Nation. Our agents, analysts, and professional staff work closely with law enforcement, intelligence, and security services—to include representatives at our Nation's airports and airlines to mitigate the threat posed to our Nation's transportation infrastructure and internal aviation security processes and systems. By combining our resources and leveraging our collective expertise, we are able to investigate National security threats that cross both geographical and jurisdictional boundaries.

CIVIL AVIATION SECURITY PROGRAM

In conjunction with our partners, the FBI's Counterterrorism Division's (CTD) Civil Aviation Security Program (CASP) is extensively involved in efforts to uncover and prevent terrorist operations to attack or exploit civil aviation in the United States. The FBI has Special Agents and Task Force Officers assigned as Airport Liaison Agents (ALAs) at each of the Nation's TSA-regulated airports in order to respond to aviation-related incidents and threats, participate in joint FBI–TSA airport vulnerability assessments, and interact with interagency and private-sector stakeholders at airports around the country on exercises, threat mitigation, and other issues to protect the travelling public.

The FBI's CASP and ALA Program were created in 1990 to formalize the Bureau's investigative, intelligence, and liaison activities at the Nation's airports. CASP is located in the FBI's National Joint Terrorism Task Force with a focus on supporting and enhancing efforts to prevent, disrupt, and defeat acts of terrorism directed toward civil aviation, and to provide counterterrorism preparedness leadership and assistance to Federal, State, and local agencies responsible for civil aviation security. One of CASP's primary responsibilities is to provide program management and support to the FBI's ALAs. In addition, CASP represents the FBI on aviation security policy matters, provides guidance and training to the field, and supports National aviation security initiatives and mandates. I would like to go over briefly CASP's efforts to mitigate the insider threat at America's airports.

INTELLIGENCE PRODUCTION

Since 2009, CASP has produced numerous intelligence products that are shared with the U.S. intelligence community. A couple of the Unclassified product titles include:

- Aviation-Related Suspicious Activities: An FBI Assessment (3 June 2005)
- Terrorist Training Document Reveals Travel Guidance and Tactics (13 October 2009)

To further mitigate threats to aviation, CASP produces and distributes a comprehensive daily aviation-centric intelligence summary for all ALAs and various FBI programs. This summary includes the latest threats to aviation, suspicious activity reporting within the Air Domain, current intelligence reporting, and updates on active aviation cases of importance. In addition, CASP intelligence analysts produce threat intelligence reports yearly in support of Congressionally-mandated FBI-TSA Joint Airport Vulnerability Assessments (JAVAs) and coordinate on-site FBI representation at JAVA events.

LIAISON

CASP has conducted three FBI Air Carrier Security Directors (ACSD) Forums since 2011, with a 3-day forum planned for August of this year. CASP has published nine aviation-centric Operation Tripwires since 2003, with a 2010 Operation Tripwire that addressed the insider threat specifically. For those of you not familiar with the FBI's Operation Tripwire, it began in 2003 as a CTD initiative designed to improve the FBI's intelligence and information base. The program's vision is to develop FBI partnerships that help to identify U.S.-based terrorist sleeper cells through collecting and assessing specific information related to potential counterterrorism threats. The program's goal is to leverage outreach programs focused on aiding industry and local officials in recognizing suspicious activity and providing them a point of contact for reporting that activity, as well as to provide actionable items for the Joint Terrorism Task Forces (JTTF).

CASP proactively develops curriculum on aviation security issues and provides training to ALAs, other Government agencies, the private sector, and foreign governments.

OPERATIONAL SUPPORT

CASP provides operational support to the FBI's ALAs and substantive units on active investigations, and provides strategic intelligence products on terrorists' tactics, techniques, and procedures. CASP responds to:

- Official Requests for Information and Requests for Assistance
- Requests related to investigations of laser pointer illuminations of aircraft
- Unmanned Aerial Vehicle incidents
- Government Accountability Office inquiries

- National Transportation Safety Board (NTSB) aircraft accident investigation assistance
- Aviation-related exercises and Hijacking Response Plans involving ALA and FBI equities.

CASP developed a series of ALA best practices that leverages division-specific initiatives for broad participation by all FBI divisions and ALAs. These initiatives include documents and guidance on conducting vulnerability assessments at General Aviation airports under the "General Aviation Assessments Initiative"; issuing Federal misdemeanors for non-felonious criminal acts at airports under the "Federal Misdemeanor Violations" best practice; conducting recurring criminal record checks through the FBI's National Crime Information Center on airport employees under the "Air Domain Computer Information Comparison" initiative; and providing checklists and guidance for handling a major aviation crisis, such as a commercial airliner crash, under the "Aviation Crisis Response Checklist" best practice initiative.

CASP also has access to the Federal Aviation Administration-managed Domestic Events Network allowing for enhanced response and situational awareness during "real-time" aviation incidents.

TRAINING

One of CASP's major focus areas is conducting training for the FBI's ALAs, other Government agencies, and private-sector stakeholders. CASP has led the way with innovative, cost savings training initiatives that include:

- In 2011, CASP conducted joint FBI-NTSB ALA Regional Training, instructing attendees on how to handle issues surrounding a major aviation crisis within their area of responsibility. Conducted three FBI ACSD Forums since 2011, and CASP launched a mandatory ALA-specific Virtual Academy Training Course for FBI employees entitled, "Airport Liaison Agent Fundamentals," in 2012.
- CASP recently worked with ALA Coordinators for in-depth training at Los Angeles International Airport, Los Angeles, CA, on 10–11 September 2014.

WORKING GROUPS AND POLICY MEETINGS

CASP represents the FBI's equities on various interagency and industry committees/working groups, such as:

- Air Domain Awareness Working Group
- Man Portable Air Defense System Analyst Working Group
- Secondary Barrier Working Group
- Civil Aviation Threat Working Group
- Aviation Information Sharing Working Group
- Air Domain Intelligence-Integration and Analysis Center Working Group
- Unmanned Aircraft Systems Event Reporting Working Group
- International General Aviation Working Group

INSIDER THREAT CASES

Several recent high-profile cases underscore the threat from "insiders," which are rogue employees that exploit their credentials, access, and knowledge of security protocols. The FBI and our interagency partners cooperated on the following arrests:

- The arrest of Wichita-based Terry Lee Loewen on December 13, 2013 by the FBI Wichita JTTF. Loewen was charged with attempted use of a weapon of mass destruction, maliciously attempting to damage and destroy by explosive, and attempting to provide material assistance to al-Qaeda in the Arabian Peninsula. Loewen, an avionics technician with Secure Identification Display Area badge access to Wichita Mid-Continent Airport, was taken into custody after he allegedly armed what he believed to be an explosive device and attempted to open a security access gate. During the investigation, Loewen allegedly engaged in, among other things, pre-operational surveillance, photographing gate access points, researching flight schedules, and assisting in the acquisition of vehicle-borne improvised explosive device components and construction of an explosive device.
- In December 2014, Eugene Harvey, a baggage handler at Hartsfield-Jackson International Airport, was arrested on a Federal complaint charging him with trafficking in firearms and entering the secure areas of the airport in violation of security requirements. The complaint alleges that Harvey repeatedly evaded airport security with bags of firearms, some of which were loaded. He then allegedly passed the guns off to an accomplice who transported them as carry-on luggage to New York, where they were illegally sold. On at least five occasions in 2014, Harvey, a baggage handler for Delta Air Lines, worked with an-

other former Delta employee to allegedly smuggle firearms through airport-controlled security checkpoints for Delta employees, and thus he was not required to go through the screening performed for passengers by TSA. Once through the airport-controlled security checkpoints, the firearms were allegedly carried in carry-on baggage into the passenger cabins of aircraft. Each time, Harvey's accomplice flew to New York with the guns, where they were allegedly illegally sold.

CONCLUSION

Chairman Katko, Ranking Member Rice, thank you again for this opportunity to testify concerning access control measures at our Nation's airports. The FBI's efforts and successes would not be possible without the continued positive working relationship with our partners and your support. I would be happy to answer any questions you might have.

Mr. KATKO. Thank you, Mr. Perdue, for your testimony.

We appreciate you both being here.

We—I know your time is valuable. I now recognize myself for 5 minutes to ask questions, and I will start with Mr. Perdue.

Mr. Perdue, in your written statements to the committee you included two examples of the insider threats that the FBI was intimately involved with during the past few years. The first one was the arrest of Wichita-based Terry Lee Loewen on December 13 by the FBI, an act of potential terrorism. The second was the Eugene Harvey case, the baggage handler in the Hartsfield-Jackson International Airport in Atlanta, who was involved in the gun-smuggling case. You are familiar with both those cases; is that correct?

Mr. PERDUE. Yes, sir. They are on-going investigations.

Mr. KATKO. Is it fair to say that both these cases point out that there are serious concerns with respect to employee access at airports?

Mr. PERDUE. I think we would concur with that, sir. Yes.

Mr. KATKO. Could you turn your microphone on?

Mr. PERDUE. Yes, sir. We would concur with that.

Mr. KATKO. Thank you very much.

Mr. PERDUE. Apologies.

Mr. KATKO. Now, based on these cases and the other cases that the FBI has been involved in with respect to employee access at airports, has the FBI developed any sort-of level of concern about this issue or do they consider it to be a major issue with serious threat or is it not a big deal to them?

Mr. PERDUE. No. It is a big deal for us. I think one of the things that we continue to do is to work with TSA and to collaborate and to come up with other programs that we think that we can help each other with the security matters.

Mr. KATKO. Okay. So you have been making suggestions to the TSA as to certain ways you can enhance the security?

Mr. PERDUE. Yes, we have. Over the last actually several months, we have had a couple of pilot projects that were literally at the ground level that we think that we can significantly enhance both of our capabilities for security at the airports.

Mr. KATKO. Could you briefly summarize some of those pilot projects for us?

Mr. PERDUE. Well, one of them without an acronym, I think it is being done at 20 different——

Mr. KATKO. Everything is done with acronyms in the Government by now.

Mr. PERDUE. Exactly. So there is a project that we have been working on, it is at 20 different airports now, that we believe that we will be able to, as opposed to doing the checks just once where we could do on-going recurring, you know, checks back with our criminal justice investigative service. So it is an on-going project. It is still nascent. That we are going to be working with TSA this year to see if we can't get that implemented at more than just 20 of the airports.

Mr. KATKO. Is there any other raw projects that you are suggesting?

Mr. PERDUE. That is the main one right now, sir.

Mr. KATKO. Now, when you are talking about doing the background check, is it fair to say that once an employee survives an initial background check and is given a SIDA badge, which gives him access to the airport, that they go back and do screening, but they don't go back and check criminal history; is that correct?

Mr. PERDUE. That is correct from my knowledge, sir.

Mr. KATKO. So just to pose a scenario to you. If someone gets arrested after being employed at the airport, you may not know about that; is that correct?

Mr. PERDUE. That is correct right now based on the situation. Yes, sir.

Mr. KATKO. That is something that needs to be addressed?

Mr. PERDUE. Indeed. That is—the prod sys that I was making reference to, I think, will greatly enhance that this coming year.

Mr. KATKO. I am used to asking questions for hours, so this is difficult to ask it all in 5 minutes. So forgive me.

But quickly switching gears, with respect to the gun case—the Harvey gun case in Atlanta, I know that the FBI wasn't in on that case from the beginning. Could you tell me when the FBI first found out that local authorities in New York City were investigating this matter?

Mr. PERDUE. I don't know the exact time, and it is an on-going investigation. We can get back to you on that, sir. We would be happy to do that.

Mr. KATKO. One of the things I would like to know is when you first found out about it and when you think you should have found out about it. Because one of the things I think we should consider here is when Federal authorities should be notified of aviation cases when local offices are doing them.

Mr. PERDUE. We would be happy to get back to you on that.

Mr. KATKO. Thank you, sir.

Switching gears here briefly, if I may. Mr. Hatfield, thank you for your testimony today, and I appreciate it. The ASAC—you mentioned that the ASAC committee has—you have met with them recently and they have given you some preliminary recommendations. Are you at liberty to share any of those with us at this time?

Mr. HATFIELD. Sir, I did in fact meet with them yesterday, first one-on-one with their Chairman, and then with the entire group. The working group is a subset of that group. We are expecting, I believe it is the end of this week, that first set of—I don't believe that they will be recommendations. But the way they described it, they will give us the, you know, who, what, when, and how, you know, where they are and where they are headed with this work.

Then at 60 days, a month from the end of this week, they will report again. Then their recommendations we expect at the 90-day mark, which would be 2 months from this Friday.

Mr. KATKO. All right. You will share those results with the committee?

Mr. HATFIELD. Absolutely, sir.

Mr. KATKO. All right. Thank you.

Mr. HATFIELD. In fact, I am as eager to get them as you are.

Mr. KATKO. Now, when we are talking about what goes on in Miami, you worked in Miami's airport. Is that correct?

Mr. HATFIELD. Negative, sir. I was the Federal security director for TSA at Miami for nearly 7 years.

Mr. KATKO. At Miami's airport. Okay. Right.

Now, when you were there, did you get any understanding of how they were able to afford it and handle doing that at such a large airport, doing full security checks for all employees?

Mr. HATFIELD. Well, they are on record as describing the price tag as just over $3 million a year. The tough thing in this answer, sir, is defining the word "it." How they did it.

So they were doing screening. They do it today. But "screening" is a word that has a broad range of meaning. So I can just tell you in short terms that what they do in terms of their screening protocols at the four employee checkpoints and at the seven elevators that have access to the secure area is a very different type of screening than what we do at the very visible checkpoints in the lobby. It is different from the type of screening we do in our random unpredictable mobile screening at employee access points.

Mr. KATKO. I would ask you how so, but I am already over the limit. So I presume if someone else could follow up with that. But last——

Mr. HATFIELD. I will talk fast.

Mr. KATKO. I am good at that, too.

The last thing I will ask you is with respect to the GAO numbers you referred to about the cost in having full screening of all employees, that was in 2008, I believe it was; is that correct? In 2009?

Mr. HATFIELD. The HSI, the Homeland Security Institute study, which puts in price tags—a range of price tag on that subject.

Mr. KATKO. That was before GSA had their PreCheck program. Is that correct?

Mr. HATFIELD. It was—that definitely preceded TSA's PreCheck.

Mr. KATKO. Do you think it would be prudent, when we are considering everything in the total mix of measures—remedial measures to take that we take into consideration perhaps a new study from GAO or somebody to see what the updated numbers might look like?

Mr. HATFIELD. I think by virtue of the fact that that is now a 7-year-old study, if we are going to really drill into this, I would not object, nor would I dissuade a new study to really look at it and try to squeeze some hard cost estimates out of it.

Again, the toughest challenge in doing that study is going to be establishing a set of definitions. Because screening—there is screening, and there is screening, and there is screening. We can't just lump it altogether as though it is sort of a universal practice.

Mr. KATKO. Yes. That is perfectly understood, and I couldn't agree with you more. Thank you very much both you gentlemen.

I am now going to recognize the Ranking Minority Member of the subcommittee, the gentlelady from New York, Miss Rice, for any questions she may have.

Miss RICE. Thank you, Mr. Chairman.

So I am going to start with you, Mr. Perdue. I want to thank you both for coming here because this is not—this hearing is not about us asking gotcha questions at all. If we are going to get to the bottom of how we can keep American travelers safe at the 450 airports we have in this country, we have to be able to have an open and frank discussion.

I have to say that, you know, obviously Mr. Chairman and I have significant prosecutorial experience in our backgrounds. I was working—you might have been, too, Mr. Chairman—but on 9/11 for the Federal Government. One of the things that came out in the aftermath of 9/11 was the lack of communication between the various agencies in the Federal Government. They were not sharing information that, had they been, some things might have been able to be addressed earlier.

So my question to you, Mr. Perdue, is: What protocols are put into place, if any, that the FBI has with not just the Atlanta airport, but any airport in this country in order to information share, whether that is investigations that are on-going that you are doing to an airport employee that you need to inform local authorities about or the reverse?

Mr. PERDUE. Yes, ma'am. That is hopefully an easy question. Since 9/11, of course, we focus on our Joint Terrorism Task Forces. So every one of our 56 field offices has, at least, one Joint Terrorism Task Force. Each of these Joint Terrorism Task Forces have at least one airport liaison agent assigned to each of the airports.

So we have roughly about 100—excuse me—about 450, give or take, you know, agents or task force officers that work for FBI's Joint Terrorism Task Forces that are at the airports every day. So collaboration, information sharing is key to everything that we do.

So I don't mean to be so short or succinct, but that is a part of what we do. We preach it, we talk about it, and we do not tolerate the lack of sharing. So——

Miss RICE. Well, it just begs the question as to why there maybe wasn't that kind of information sharing in the case that we are talking about in Atlanta?

Mr. PERDUE. Yeah. I do not have the details on that. I will say that that was a criminal investigation, and it is not that our criminal program is not as tight as our counterterrorism program. I would not suggest that. But I would say it is two different, you know, sets of work, even though that we do work collectively together at the airports.

So we can get back to you on that, ma'am, on the details of that investigation. I don't know what actually fell apart at the time.

Miss RICE. So there is no legal prohibition from the sharing of information. Correct?

Mr. PERDUE. There is not.

Miss RICE. Confidentiality or——

Mr. PERDUE. No, ma'am.

Miss RICE. Okay. So I don't think there is any question that we need to do more robust criminal background checks.

Is there anything preventing, from a logistics standpoint, going back ad infinitum? Forget about the 10-year barrier. Doing a lifetime criminal background check, going back to whenever the person may have first had contact with the criminal justice system. Is there anything preventing that from being the way we conduct criminal background checks?

Mr. PERDUE. I don't know the details. I don't know how cost-prohibitive it is. I know the TSA has some details on that.

I would say, though, that the pilot project that we are working toward hopefully we will get access 24/7 to the Criminal Justice Information Center, CJIS, at Clarksville for TSA and that information.

So I think we have this pilot, and we will be looking at other pilots this year, where we can make our information readily available to them and in a system that would not be cost-prohibitive.

Miss RICE. All right. Do you know what the rationale is for only going back 10 years?

Mr. PERDUE. I do not, ma'am.

Miss RICE. So you do do recurrent criminal background checks now? Is that true?

Mr. PERDUE. No. There is a—I think at 20 of the airports right now, we have a pilot project that we are working on. So the goal this year is to enhance that.

Miss RICE. Now, it is—correct me if I am wrong, but it doesn't require anything other than just looking, I guess, refreshing the review of a set of fingerprints to any number of databases. Correct?

Mr. PERDUE. The fingerprints would be one and, of course, just setting up a system where the information could be, you know, passed readily. So, again, that is something we will be working with TSA on this year.

Miss RICE. So is there any way that you can set up a system of information sharing whereby an airport employee gets arrested, does not share that information with their employer, but a law enforcement agency can share that with the airline or the TSA?

Mr. PERDUE. Yeah. That would be at the heart of this pilot project. So——

Miss RICE. That is the heart of it.

Mr. PERDUE. So that would literally be at the heart of it.

Miss RICE. What is—what obstacles are in the way? I mean, do you see that as do-able?

Mr. PERDUE. I think—I think so. It is do-able. We have had discussions about this over the last couple of days, and we will be pursuing it, and we will look forward to testifying about it later.

Miss RICE. Okay. So, Mr. Hatfield, I have a couple of questions for you. So when you are driving to work in the morning and you are looking at the day ahead of you, answer this question for me: The top three things that are going to frustrate me today in terms of enabling me to get my job done are?

Mr. HATFIELD. Well, that has to start with the word bureaucracy. Let me answer that, if I can, quickly in three ways. Inside: Our business is a people business. We have 60,000 employees, and 43,000, in round numbers, are in uniform. We do what we do with technology, but the heart of our efforts are the people. So hiring those people, retaining those people, teaching, training, and cultivating those people can sometimes be a challenge with the personnel rules that we have to deal with. Getting rid of the bad people, the ones who don't belong there, is probably the most frustrating process that we go through. It can be very lengthy in the Federal system.

That said, I have been here for about a week and a half at headquarters in from Miami. In my new role, I am very encouraged by the briefing that I just had by our human capital director, who is taking real aggressive steps towards streamlining, hiring, toward making the process, the Federal personnel processes easier for our field leaders, our Federal security directors to follow.

Outside, you know, in the big picture, I see the faces almost every day in intelligence briefings of the suspects, the known individuals who are plotting, planning, or suspected of planning terrorist acts.

I can tell you, I have been for almost 13 years in this agency, my sense of urgency, my commitment, my belief in the reality of that threat is more real today than it was when I started in 2002. Making sure that everyone else has that urgency, it can be frustrating. You know, the longer we go from any major domestic event, the shorter people's memory retention and the thinner it gets. We have a lot of stakeholders, we have a lot of customers, we have a lot of employees. Making sure that everybody shares that sense of urgency or, at least, that recognition of how real the threat is. They don't have to all be as urgent as we are at the center of the storm, but let's make sure we don't dismiss this threat as something that went away, because it did not.

Miss RICE. Mr. Chairman, if I could just be indulged for one more brief second.

You talked about the difficulty in terms of defining screening. You are well aware of the program that Miami has in place. You have actually lauded it and said it is, you know, basically like a blue ribbon system.

Regardless of how you define screening, in your opinion is there any amount of money that is too much to ensure the safety of Americans traveling on our airlines?

Mr. HATFIELD. You know——

Miss RICE. Is there a logistical impossibility? You have to keep it very brief. But is there a logistical impossibility to implementing them at various degrees depending on threat assessments that are made at each individual airport so that the cost can be contained and the actual threat can be addressed?

Mr. HATFIELD. I am going to take that in three parts and try and be as quick and responsive as possible.

No. 1, the Miami system, absolutely laudable. Blue ribbon in the initiative that it represents and the willingness to take on unilateral cost, expense, and activity that the airport has demonstrated now for many years. It is a good system for airport crime fighting, theft, smuggling, the kind of things that it was designed to do. It has collateral benefit for counterterrorism work. But that is not its primary design, nor is that a primary, you know, part of the whole mix there.

On the cost piece of it, that is a tough discussion to ever get into. I will answer it this way: I want to be better every day. Better does not always mean more, more money, more time, more resources. Better means better. Better means looking at your vulnerabilities that are highlighted through public disclosures, through your own self-analysis towards your own assessment—by your own assessments, and demanding better of yourself and your people every day.

Miss RICE. Thank you.

Mr. HATFIELD. There was a third point, and I apologize——

Miss RICE. Thank you, Mr. Hatfield. Thank you, Mr. Chairman.

Mr. KATKO. Thank you very much.

Now, in accordance with our committee rules and practice, I plan to recognize Members who were present at the start of the hearing by seniority on this subcommittee, alternating back and forth between my right and my left.

So the next person up is the gentleman from Alabama, Mr. Rogers. I give you 5 minutes. I will note, Mr. Rogers and the others on the committee, we have been a little lax on the time, but we are going to have to enforce it a little more strictly going forward.

Mr. ROGERS. Thank you, Mr. Chairman.

Mr. Perdue, the Ranking Member was asking you about the data collection and the background reviews. You mentioned fingerprints.

Are there some other points of data that could be collected that aren't currently that you think would be helpful in that 10-year or whatever number of years review?

Mr. PERDUE. Well, the Criminal Justice Information System out at Clarksville, of course, it has the biometrics, so there is fingerprints, there is other biometrics, and there is just literally all of the thousands and thousands of points of information that we collect in our intelligence programs.

So, with the speed of computers, all we would need to do is obviously, you know, access that and to run checks against it. So other than——

Mr. ROGERS. The data being collected is adequate. You just——

Mr. PERDUE. I believe so. The whole idea, I think, is to create a functional system where we can exchange it, you know, freely and openly in a timely manner.

Mr. ROGERS. Thank you.

Mr. Hatfield, to follow up on the Chairman's questions. In Miami, you kind of left it. You said you will talk faster. But tell me more about how the Miami system works. I think you said there is four points of entry for the employees?

Mr. HATFIELD. Gladly. The basic story to be told here is that back in 1999, to face a rash of theft issues and smuggling, they looked at how they could tighten up controls, access controls with employees.

The first thing they did is something that every airport in the country can do today, that many have done over the years because it is a dynamic, evolving industry, and that is how many access points are there? Pedestrian, vehicle, or combination.

If you reduce that number of access points, you reduce the opportunity. You are also able to better focus and better train your resources on securing those points of access and egress. So the screening itself, the most robust part of it, is at four choke points. I think that at one point they had nearly 40 access points. They have a fraction of that now, both for vehicles and for people.

They have a traditional set-up with a magnetometer, walk through a metal detector, and an X-ray machine to screen both people and their bags for metallic objects, metallic threat items. So this is a guns and knives, the kind of classic items. But the—you know, there is a whole range of dynamic differences between that and the screening upstairs.

Again, I can't say enough good things about what they have done in Miami. In the years that I spent down there, they were absolutely engaged partners, as were every other member of that airport community. I didn't get a chance in the beginning, but Mr. Perdue's folks at each airport I have worked at, Newark, Kennedy, and Miami, have been very strong partners for us. He certainly is a representative of the kind of quality individual that the FBI joins and partners with TSA day in and day out across the country.

Mr. ROGERS. So this does not sound like an overly burdensome process at those four checkpoints for the employees in Miami. But yet you seem to indicate that you didn't think that would be a system that would work at other airports. Did I misinterpret?

Mr. HATFIELD. No, sir. I didn't venture a speculation on that. I think that what was replicable—what is replicable at other airports is that first step that they took when they started this initiative many years ago, and that is look at how many access points there are for both people and vehicles, and what can you do to continue running the airport, maintain operations and efficiency, but reduce the number of opportunities.

Mr. ROGERS. Assuming that each airport did that, would you not agree that it would not be overly burdensome to require employees every time they reenter a workplace to go through a magnetometer?

Mr. HATFIELD. It goes to a more fundamental question, sir. That is we look at the screening of the employee base in this context. It is a known and trusted population. So through the vetting, through the credentialing——

Mr. ROGERS. There was that fellow in Atlanta that brought the guns back and forth——

Mr. HATFIELD. Right. It doesn't end with vetting and credentialing. It has to include a physical screening component.

Mr. ROGERS. So the answer is, yes, that is not an overly burdensome requirement to require every employee that comes back into the workplace to go through a magnetometer?

Mr. HATFIELD. It is not an overly burdensome requirement because it happens today. TSA does most of it. But airlines and airports also do physical screening in addition to Miami. Now, they are the example of 100 percent, and I believe Orlando has been mentioned as well.

Mr. ROGERS. Well, my point is requiring 100 percent of the employees would not be an overly burdensome requirement, just to go through a magnetometer.

Mr. HATFIELD. I think that for the best answer to that, I would wait for the report back from the ASAC, the security advisory group, because they are really doing a deep dive into this, and they have got the representation of all of the key stakeholders and players, as well as TSA participation in that group effort.

Mr. ROGERS. Well, I don't need to wait for the report. I know what the answer should be.

With that, my time has expired. I will yield back, Mr. Chairman.

Mr. KATKO. Thank you very much, Mr. Rogers.

The Chairman now recognizes Mr. Thompson.

Mr. THOMPSON. Thank you, Mr. Chairman.

Following along Mr. Rogers' line of questioning, Mr. Hatfield, who is tasked with the responsibility for this committee's information once a person is credentialed? Who is responsible for making sure that that person is who they are as it relates to going to work every day?

Mr. HATFIELD. I apologize, sir. I didn't quite hear the middle part of that question.

Who is responsible——

Mr. THOMPSON. Well, once a person receives a SIDA badge——

Mr. HATFIELD. Yes.

Mr. THOMPSON [continuing]. And goes to work, is that the airport's responsibility for guaranteeing that that person is who they are, or is it TSA overseeing the process that the airport does?

Mr. HATFIELD. It ultimately falls on both. It starts with the airport because the airport is the entity that collects the information necessary to submit to TSA for the criminal history record check and for the security threat assessment. That information includes fingerprints and personal identifiers. For the airport's purpose, they may or may not collect Social Security. But they do then send that to TSA. We do the check and send back the results.

As far as maintaining—you know, that was one that was a recent study not long ago.

Mr. THOMPSON. So—so—I understand. I am trying to get——

Mr. HATFIELD. Sure. Go ahead.

Mr. THOMPSON [continuing]. Everything down. So once that person has the badge——

Mr. HATFIELD. Yes.

Mr. THOMPSON [continuing]. For 10 years, there is no review, or what is the review?

Mr. HATFIELD. The review is on a continuous basis on the TSA security threat assessment side because what happens is that name—those identifiers go into a database that is continually checked against the Terrorist Screening Center's database. The question at hand——

Mr. THOMPSON. But not the criminal.

Mr. HATFIELD. No, sir. That is the question that is before the ASAC.

Mr. THOMPSON. Not criminal, but terrorist. The burden is on the airport to guarantee that that person is who they are?

Mr. HATFIELD. Yes. It is. When they collect their information, they have a process to——

Mr. THOMPSON. How about going to work every day? When that person goes to work every day?

Mr. HATFIELD. In terms of matching the ID with the face, many people are involved in that, sir. Most airports have challenge programs; if you see somebody on the ramp who is not showing an ID, if you see somebody on the ramp and use testers who wear a woman's ID or——

Mr. THOMPSON. But who is ultimately in charge of the program? Is it the airport?

Mr. HATFIELD. Of the program of verifying identity on a daily basis? Everybody in that airport community is responsible for it.

Mr. THOMPSON. I understand, but I am—I am a ramp worker——

Mr. HATFIELD. Okay.

Mr. THOMPSON [continuing]. Going with my SIDA badge. If something happens, is it the airport, or are you saying it is everybody working together has to figure out who is there?

Mr. HATFIELD. You are getting to your job on the ramp, and it is in a secure area. You use that badge and you swipe through a reader or you present it to a guard, or, in some cases, you go through a screening area, but in fact that——

Mr. THOMPSON. I am trying to narrow the area of responsibility so that we kind of understand, because I am trying to get to the other part of the question.

Who pays for that? Is it the airport that pays for the screening of those individuals, or is it who?

Mr. HATFIELD. Sir, that is a complex question with a complex answer. So the easy part of that is who pays for the screening? Well, if they go through my checkpoint at Miami, I am going to screen them and TSA pays for it. If they go through Miami's checkpoint, the airport pays for it. If you go to Atlanta, they also pass through the TSA checkpoint which I guess the cost is then borne by TSA, but they go through—they go through a Delta screening contractor when they get on an employee bus.

Mr. THOMPSON. So there is no one entity.

Mr. HATFIELD. There is a combination, sir.

Mr. THOMPSON. So there is no one entity in charge?

Mr. HATFIELD. There are—well, leadership is shared and command is shared.

Mr. THOMPSON. I understand. The individual with a SIDA badge, who is responsible for keeping up with the badges?

Mr. HATFIELD. The airport security office is responsible for the issuance and the retrieval of those badges——

Mr. THOMPSON. All the badges.

Mr. HATFIELD. Yes.

Mr. THOMPSON. So do you require a monitoring of that process?

Mr. HATFIELD. Absolutely, and, in fact, we have responded to a recent Government study that said there needed to be tighter constraints on that, and I was not here at headquarters when that took place and was delivered, but I was in the field, and I can tell you it manifested itself at the Miami security office in terms of how they audited, managed, retained records——

Mr. THOMPSON. So are any of those SIDA badges, to your knowledge, biometric?

Mr. HATFIELD. I am sorry, sir.

Mr. THOMPSON. Are any of them biometric?

Mr. HATFIELD. In Miami, they are not. Biometrics are the—up to the discretion of the airport in terms of selecting, purchasing, deploying biometric reading equipment.

Mr. THOMPSON. To your knowledge, do you know any airports that use biometrics?

Mr. HATFIELD. I know that some do, and I can't—I can get you names of them. We will poll them.

Mr. THOMPSON. Please get us.

Mr. HATFIELD. Okay. You want it for biometrics for——

Mr. THOMPSON. Your indulgence, please.

Mr. Perdue, are you aware, in line with the Ranking Member of the committee's questioning, aware of any written protocols for the sharing of information with either airport police—and I am trying to get to the Atlanta situation. Would the Atlanta airport police department have been involved in a situation like that, or would that investigation have been conducted outside that airport?

Mr. PERDUE. I am not for sure I understand the question, sir, but——

Mr. THOMPSON. Well, you have New York and Atlanta involved. I am trying to see at what point are there written protocols that would bring the Atlanta airport authorities, police or whomever, into this investigation since it went on so long. Would it have been at the beginning, in the interim, or at the end?

Mr. PERDUE. If the FBI had been in charge of it, sir, hopefully what we would have done would, and what we do with all our other investigations, we share, we collaborate and we do our best to make sure all of our partners know what is going on, and so on the particular issue, the question was is that am I aware of a written protocol that oversees local police officers sharing information? I am not, sir.

Mr. THOMPSON. Not local. Federal sharing information with locals. The other way.

Mr. PERDUE. Inside the FBI, I am aware of the FBI's, you know, guidelines, our policies, and that they are all about sharing and collaborating, sir.

Mr. KATKO. The Chairman recognizes Mr. Carter.

Mr. CARTER. Thank you, Mr. Chairman.

Mr. Hatfield, not to be redundant, and forgive me if I am, but I just want to make sure I understand this and I have got a clear understanding of it is that the SIDA cards that are issued at one airport are not—are not valid in other airports.

Mr. HATFIELD. Right.

Mr. CARTER. Okay. At a certain airport, such as Atlanta, at Hartsfield, that the list is maintained by the airport authority of those people who have the SIDA badges.

Mr. HATFIELD. The list of SIDAs, yes.

Mr. CARTER. SIDAs, okay. Is it ever—do they ever review it and just randomly check them? I know that you mentioned that they check them against the terrorism threats and such, but do they just have random checks from time to time?

Mr. HATFIELD. Some airports do, sir. I know, in fact, coming back to Miami, Miami does that. The Miami Police Department—Miami Dade County Police Department will go into the security office on a periodic basis, and it is pretty frequent, and they will take a chunk, a representative sample, and they will go back and they will run a recurrent criminal history record check against it, but, again, that is their initiative. It is not a requirement.

Mr. CARTER. Okay. Why isn't it a requirement? Why don't we have more consistency among the airports?

Mr. HATFIELD. It is a good question in terms of why isn't it a requirement. The part of the work that we are doing collaboratively with the FBI right now is to come up with a means to do it. So we have got a mechanism, and it is a fairly new mechanism that allows us to do recurrent vetting against the terrorist database to do terrorist database screening. It is not just something that is existing that can plug and play, which is why we are developing it, and I think we are fairly on the record, if we are not, I guess I am on the record now, we are looking for that. We want to be able to do constant recurrent criminal history records checks.

Mr. CARTER. Okay.

Mr. HATFIELD. We can go to the Ranking Member's question of the duration how far back we look, that is a separate issue, but in terms of do we want a mechanism that can allow us to do the same thing with criminal history records that we do with the terrorist database? Yes, sir.

Mr. CARTER. Okay. Let me ask you this: What did we learn in Atlanta?

Mr. HATFIELD. We were reminded in Atlanta of the fact that our airports are open and to a degree knowingly porous facilities. They—that is part of being an airport, that there are vulnerabilities. That it is our responsibility to identify and address those vulnerabilities, but just as important as identifying and addressing the vulnerabilities is understanding the threat and what the two of those things together go to create a risk.

So the demonstration that that gun-running operation did was it was—it was a glaring vulnerability in that case. I wouldn't say that it was in and of itself a brand new revelation. We know that crime takes place in airports like it takes place in cities. They are just—they are smaller cities, and so we need to—you know, that is part of our partnership with the FBI and with local and Federal law enforcement is there is crime fighting that is going on in airports across the country, and there is counterterrorism work. We do overlap. We each benefit from each other's work, but they are separate disciplines, and so in that combined effort, we need to maintain focus on both of those challenges, and, again, what did we learn? I think we learned what I said earlier. We can do better. I think we can challenge ourselves to do better. Is that answer 100 percent employee screening? I don't know that it is. Again, I am eager to hear the council—ASAC's recommendations, but I do think that today now, even before those recommendations come in, we have taken steps that are helping us do better increasing employee screening.

Mr. CARTER. Okay. I know that there are a number of agencies, as you have alluded to, that have a part in this, but I want to concentrate primarily on airlines. What is their responsibility, and if they fail at that responsibility, is there any kind of disciplinary action or anything?

Mr. HATFIELD. I will be honest with you. The requirement for them to do employee screening is open to interpretation. It is fairly broad. So in some cases, you will find airlines—Delta is included in Atlanta, by the way—where they are paying a third-party contractor, a security force provider, to screen their employees at points prior to entry into the secure area. They are footing the bill and executing that security measure on their own dime. That takes place in airports around the country by various airlines. So there is a commitment out there. There are demonstrable examples of it, but it is not a—there is not a cut-and-dry standard or a threshold, a percentage, a number that they have to adhere to.

Mr. CARTER. Do you feel like there should be?

Mr. HATFIELD. The difficulty in doing that is, as Mr. Thompson said, there are 450 airports out there. We have got 80 Federal security directors who, through a system of hub and spokes and standalone airports, work to create a tailor-made custom security plan for each of those airports. They demand that. So we might be able to get more specific. I think that is one of the things that we are looking at with the ASAC in terms of setting those screening goals for what the airport or the airlines are responsible for, but I am not going to pre-empt their recommendations in that.

It is a cookie-cutter standard, a target number, a 10 percent or 1,000 or any of those I think would be impractical, but we are good at working on these custom solutions. We have got Federal standards, and we know how to apply them in 450 different areas. So this could be one of those things that we learn how to change our behavior with.

Mr. CARTER. Thank you very much.

Mr. KATKO. Thank you, Mr. Carter.

The Chairman now recognizes the gentleman from New Jersey, Mr. Payne.

Mr. PAYNE. Thank you, Mr. Chairman, for having this committee hearing.

Also to the Ranking Member of the full committee and the Ranking Member of the sub. It is an honor for me to have joined this committee.

Mr. Hatfield, being from the 10th Congressional District in the State of New Jersey, Newark Airport is 5 minutes from my home. You know, you stated in your testimony that through the security threat assessment, you know, bad actors are weeded out.

What is your response to media reports that an individual that had been issued a SIDA credential in the past was found to be fighting overseas with ISIS?

Mr. HATFIELD. I actually think that is a good example of the system that we do have the constant recurring vetting on. I believe the case you are referring to involves an individual who was identified, but he—it was after his employment in the airport that his association with ISIL had begun, and so the idea of having—look, we don't have an enemy that fosters and cultivates cradle-to-battlefront operatives. They are out there recruiting adults and, you know, people who have lived lives and, you know, can become influenced by the rhetoric and the recruiting. So you may have somebody who has had a fairly uneventful life with no criminal record, with no terrorist contact or suspicion, who suddenly becomes activated or inspired, as the magazine's title intends it to do. So that is why we believe very strongly in maintaining that constant terrorist database vetting and why that proves a good model.

Frankly, I think that there is, in this case, even higher value in that work that we are already doing, but it certainty supports our search and our work with the FBI in coming up with a constant criminal revetting system.

Mr. PAYNE. Well, let me ask you, then, once, you know, a security breach occurs, following the Ranking Member's questioning, who is responsible for reporting the breach to the TSA, and are the breaches collected into a database?

Mr. HATFIELD. Yes. They are collected into a database, and we have—it kind of depends on the nature of the breach, where it occurred, who was on site, but there is very demanding reporting requirements. You know, in a typical situation, it is TSA and the local PD of jurisdiction who are the first to get it. On our side, it will typically be our regulatory folks. It can be the screening folks or our law enforcement arm, but the local police, then, and if it rises to the level of a Federal investigation, the FBI is brought in and so forth and so on, but your typical sort-of first reporting points for an airport security incident, TSA and the local police department.

Mr. PAYNE. Mr. Perdue, you know, if a SIDA badge holder is convicted or found to be guilty of one of the 28 disqualifying crimes, are they expected to self-report the criminal activity, or is there a system in place to collect this data as well? Can you describe this process?

Mr. PERDUE. The process in place right now, again, is just when the entry-level employee's name trace and then the name checks come by through the Criminal Justice Information Center. So, other than what I have already provided testimony on today with this pilot project, those are the two things that we are working on.

Mr. PAYNE. So it is identified, or are they obligated to self-report?

Mr. PERDUE. It is not—I have no information that they are obligated to self-report, and so that would be a TSA question, sir.

Mr. PAYNE. Okay. You know, what penalties exist for those who misuse their SIDA credentials to enter a secure area of an airport?

Mr. PERDUE. I am not familiar with the exact exposure or what the crime actually would be. I defer to TSA or that too, sir.

Mr. PAYNE. Mr. Hatfield.

Mr. HATFIELD. If it is a case of misuse where there is a regulatory or a rule violation, they can face suspension or revocation of that badge, which in many or most cases means their inability to work. So there is as high price there. If it moves into a criminal act or there is criminal elements to the case, then, of course, local PD and/or the FBI or the law enforcement agencies would—and that would be a case for the court systems, depending on if prosecution resulted from it.

There also is the potential for civil penalties. Again, if it is a regulatory infraction, TSA can issue a civil penalty to an individual.

Mr. PAYNE. Thank you.

Mr. HATFIELD. You are welcome, sir.

Mr. PAYNE. Mr. Chairman, I am going to show restraint and yield back the balance of my time.

Mr. KATKO. Thank you very much.

The Chairman now recognizes Mr. Ratcliffe of Texas.

Mr. RATCLIFFE. Thank you, Mr. Chairman.

Thank you, Mr. Hatfield and Mr. Perdue, for being here today and for providing your insights and clarity on airport security measures.

I do want to follow up on the line of questioning from the gentleman from New Jersey about security breaches a moment ago, and I will direct this to you, Mr. Hatfield.

According to a DHS OIG report that was released back in May 2012, TSA is supposed to document all security breaches locally at each specific airport, and that is supposed to be done through TSA's tracking system, the PARIS system, the Performance and Results Information System. That IG report, though, found that more than half of the breaches weren't actually being reported into the PARIS system, and of those that were reported, only half of those was any corrective measures taken. So can you comment on that and, in so doing, hopefully talk to us about what reforms TSA has made to those policies and procedures to ensure that everything is being accurately reported.

Mr. HATFIELD. I can, sir. The fundamental problem at that point in time—and I will talk to the remedy since then—the fundamental problem was in the definition of "breach." You could go talk to 80 different Federal security directors or their staffs. Sometimes the most insignificant incidences were being called a breach, and other times more appropriate incidents were being called breaches. So we set out after that report and in concert with the IG, who I believe validated the response that we made, and that is to set a more defined set of parameters for what constitutes a breach.

I was in the field during that time, and I know that, you know, we worked very hard to discern between a security event—and that is sort-of—that is what we are left on the other side of the ledger, security events. They happen every day. But a breach is a pretty distinct event in itself and requires a threshold to be met. So once we got the definition down, I think our reporting through PARIS has gotten much better.

When you talk about the absence or the lack of consequences in a large number, again, you had things being called breaches that either didn't draw or demand a punitive action or were such fleeting events that there really weren't even perpetratorial players to identify in it going back. So I think that we are pretty aggressive in terms of using the regulatory weight, if you will, of the civil penalty. Of course, in most cases—and I think any good regulator follows this philosophy—corrective action and remedy to the bad behavior or the omission is the first goal rather than just, you know, collecting money for the Treasury, but if there is a repeat offense or an unwillingness to remedy and correct the problem, we absolutely will not hesitate to level civil penalties. We absolutely will not hesitate to bring in law enforcement if there is any indication of criminal activity.

Mr. RATCLIFFE. Okay. Thank you, Mr. Hatfield.

So I know there is not a subsequent IG report, but you referenced their sort-of follow-up with you in terms of recognizing with a new definition, if you will, of what constitutes a breach.

Can you put a percentage on the number of breaches that are now recorded in this system or give me an estimate of that?

Mr. HATFIELD. I don't have that visibility on the overall system, sir, but I will get back to you. I want to validate what I represent in terms of our remedy and the IG's reaction to it. I want to make sure that I have got that right. This is—at this level, sort-of an enterprise level of these activities, I am fairly new on the scene, but I have certainly seen it from the field perspective and have been part and parcel to the old practice and the new practice, and be more than happy to get you some feedback on that.

Mr. RATCLIFFE. Okay. Very good.

Mr. Perdue, I don't want you to feel left out, so I have got a math question for you too. This relates to joint vulnerability assessments. So data that I have seen from the GAO indicated that from 2004 to 2011, JVAs had only been conducted at about 17 percent of TSA-regulated airports. Now, I am not math major, but does that mean that 83 percent during that period of time weren't being assessed?

Mr. PERDUE. I do not track that or monitor that. That would be a TSA question. We participate, you know, in this and we—jointly we do these assessments, but as far as the numbers, I wouldn't have the answer to that, sir.

Mr. RATCLIFFE. Okay. But so maybe you can answer this question: Can you relate, since you do work with TSA with respect to that, and how do TSA and FBI decide which airports are going to be assessed or undergo a JVA?

Mr. PERDUE. Again, what we do is that we participate in 100 percent of them. TSA decides which ones they are going to go to and then we make sure that we have representatives there to provide appropriate threat assessments.

Mr. RATCLIFFE. Okay. Can you expound on that, Mr.——

Mr. HATFIELD. Certainly. I would be happy to. The identification of those airports, I can give you the actual numbers in closed session, but let's say, by number, it is a small amount; by volume a percentage of daily passenger traffic, it is a huge amount. So 450 airports, if you look at our smallest airports, it is nearly 300 of them, represent just a fraction of the daily passenger traffic. So we are really focused on a critical number of highly important high-traffic airports. That said—and the cycle for that is one-third of them every year. So, in a 3-year cycle, we will get back to the first set of them.

However, every single year every single airport goes through a TSA regulatory assessment. So our folks are out there looking at vulnerabilities, looking at compliance, looking at all of the aspects of the airport security plan for every single airport. That is an annual requirement, and it is a very large part of what our regulatory group does.

Mr. RATCLIFFE. Terrific. Thanks, gentlemen.

I yield back.

Mr. KATKO. Thank you, Mr. Ratcliffe.

The Chairman recognizes Mr. Johnson, the gentleman from Georgia.

Mr. JOHNSON. Thank you, Chairman Katko and Ranking Member Rice. I want to thank you for allowing me to be here today.

I sent a letter to the full committee and the Transportation Security subcommittee at the beginning of this Congress requesting that this committee hold a hearing on this very topic, and I thank you for listening to my call.

This is an important issue for National security and for my hometown of Atlanta. I made a pledge to the people of Georgia that I would focus on this issue, and it is in that spirit that I appear here today.

I look forward to working with all Members of this committee, which has important jurisdiction to protect the health, safety, and welfare of the public who transport themselves on the airlines, and this is critical work.

I want to congratulate you both for ascending to these important positions on this important subcommittee, and I look forward to working with you in the future.

As we all know, in December, at Hartsfield-Jackson Airport in my home State of Georgia, the busiest airport in the world, an employee and his co-conspirator, a former airport employee, were arrested for smuggling guns onto airplanes. If this is happening at one of—at the world's largest most prominent airport where passenger security is at the forefront, then I am afraid to think of what may be happening at other airports.

The incidents at Hartsfield-Jackson should be a wake-up call to this committee and to airports and airlines. We must ensure that airport and airline employees who enjoy unique access to airplanes undergo rigorous security screenings in order to prevent such a more serious incident from occurring, and that is not the first incident of that nature to occur at Hartsfield-Jackson over the years.

Mr. Hatfield, I heard you say before I left that random screening of employees is just as effective as 100 percent screening of employees. Is that correct?

Mr. HATFIELD. Sir, I—those were not my words. I was quoting a study, actually. It is not my conclusion. I mean, I did say that quoting the Homeland Security Institute's study, and I also qualify that by saying that even in their own footnotes, they acknowledge that they had a small sampling, and to the Member's question earlier, would it be a good idea to revisit that study, after 7 years, probably so.

Mr. JOHNSON. If the premise or the conclusion of that study, as you have stated, is that random screening is just as effective as 100 percent screening of employees, then would you not think that that same general rule would apply to airline passengers? In other words, if we don't screen 100 percent airline passengers and we just do a random screening process for them, you would not agree that we should do that. Is that true?

Mr. HATFIELD. Sir, I would not subscribe to that notion, but I will also tell you that in the 12½ years TSA has been doing this, we have evolved on the passenger side as well, and now we actually segment the population of passengers and people on the plane, including flight crew and aircraft crew. In some cases, the known crew member, we are doing primarily identity screening. So it is a different type of screening. It is not the physical screening at the checkpoint although they are subject to that on a random basis.

So, no, I would not, again, subscribe to the idea that we change our paradigm because I think we are pretty satisfied with it.

Mr. JOHNSON. But you would be reluctant to be change in terms of going to a 100 percent screening of airline employees?

Mr. HATFIELD. Again, “screening” is a big word and it has a lot of meanings. Right now we do 100 percent screening of airline employees in that we screen them against a terrorist database every day. We screen physically——

Mr. JOHNSON. Physical screening.

Mr. HATFIELD. Physical screening? Right now we physically screen about 100,000 employees a day through various means.

Mr. JOHNSON. You have got how many employees in Atlanta? About—what—40,000 if I recall?

Mr. HATFIELD. In the total airport population?

Mr. JOHNSON. Yes.

Mr. HATFIELD. I have heard it is around 40-plus thousand.

Mr. JOHNSON. That is a lot of individuals coming through, some of whom are not screened at all. But statistically you would support the notion that it would be unnecessary to ramp up screening. Is that what you are arguing?

Mr. HATFIELD. No, sir. My position is this. We have a very qualified and dedicated group who is looking at this from a very analytical point of view with broad representation of all the players in the airport community.

As an aside, I spoke with the Federal security director in Atlanta yesterday, Mary Leftridge Byrd, who is not only a colleague of mine but a friend, and talked to her about this subject. They have taken moves to ramp up the number, the percentage of physical screenings that they do as a sort-of a surge posture during this analysis while we look at what the long-range posture will be. But, again, as we bring in all the members of this community, airlines, airport operators, the TSA, law enforcement at both the Federal and local level, it is a question that demands discussion and that we are looking at.

I am not prepared, sir, today to preempt the ASAC’s recommendations nor to make conclusions at this point. But I will grant you this, yeah, we need to look at this. You know, is it going all the way to 100? Is it going to an incremental increase and the percentage that we physically screen today? I think the answer is somewhere in there.

Mr. KATKO. Thank you, Mr. Johnson for your questions.

I want to thank the gentlemen, Mr. Hatfield and Mr. Perdue. It is obvious that you are fine public servants and that you are highly competent and qualified to answer these questions. We definitely had the right people here today with respect to you two. So thank you very much for your time, and I wish you well and look forward speaking to you in the future.

Members of the committee may have some additional questions for the both of you. I will ask that you respond to these questions in writing in a timely manner. The hearing record will be held open for 10 days with respect these two witnesses.

We will take a very brief recess so that the next—the second panel can get prepared to testify.

Thank you, gentlemen.

Mr. HATFIELD. Thank you, sir.

[Recess.]

Mr. KATKO. Good afternoon. Before we get into introductions here, I want to make a couple of technical notes for the record. First from Miss Rice.

Miss RICE. Mr. Chairman, I ask unanimous consent that this letter from President Williams of AFGE Local 554 in Georgia regarding his concern over the firearm smuggling incident at Atlanta Jackson-Hartsfield Airport be entered into the record.

Mr. KATKO. Without objection, so ordered.

[The information follows:]

LETTER FROM L.P. ROBERT WILLIAMS, AFGE LOCAL 554 TSA GEORGIA

Honorable BENNIE G. THOMPSON,
Ranking Member, Committee on Homeland Security.

DEAR CONGRESSMAN THOMPSON: I am writing to express my deep concern over the recent public revelations of current and former Delta employees smuggling 131 firearms and ammunition aboard Delta flights between May 1 and December 10th 2014. This information was not surprising to the TSA Officers who work at Atlanta Jackson Hartsfield Airport.

I represent all the TSA officers in the State of Georgia and this huge glitch has been repeatedly pointed out to local supervision and management over the last three years. TSA'S Local management's would refer me back to our collective bargaining agreement that prohibits any discussion dealing with security policies, procedures and deployment of security personal. The officers who commit to protecting our homeland are discouraged and prohibited from pointing out areas where the airport is vulnerable. Developing innovative countermeasures are frowned upon when officers suggest possible fixes to the insider threat problem.

Many officers work in an environment where they believe their safety and the flying public's safety is put at risk by sequestration and staffing shortages. Atlanta's has a number of employee entrances that would benefit from increased TSA staffing who have the ability to search all airline personal more frequently. If and when that mandate is authorized TSA does not currently have the staffing to accomplish that mission.

Since the discovery of this problem in late December the PLAYBOOK team has increased it's screening of employees that enter the airport which is commendable, however it does repair the root cause of the problem. Without securing the North and South CIDA badge access doors where any current or former airline employee with nefarious intentions can enter, the insider threat has not been stopped. The only significant change is the airport vendor employees have had their ability to enter those doors taken away by the airport authority. Airline employees still have the same CIDA access.

AFGE believes the officers who are tasked with securing a port of entry to our nation should be at the table during these conversations on how best to secure the homeland. We would like Congress to encourage our inclusion in these meetings. AFGE would also like Congress to know that the taxpayers have invested millions of dollars in equipment that sits unused because TSA has not hired anyone to fill the many vacancies we have at the Atlanta airport. In closing we believe there are many opportunities to improve the security to our homeland, eliminate staffing shortages, and improve internal communication at the world's busiest airport. AFGE LOCAL 554 stands ready to serve when called upon.

Respectfully Submitted,

L.P. ROBERT WILLIAMS,
AFGE Local 554 TSA Georgia.

Mr. KATKO. I also ask unanimous consent to insert in the record a statement from Airports Council International—North America, as well as a letter from the American Association of Airport Executives.

Without objection, that is so ordered as well.

[The information follows:]

STATEMENT OF KEVIN M. BURKE, PRESIDENT AND CEO, AIRPORTS COUNCIL INTERNATIONAL—NORTH AMERICA

FEBRUARY 3, 2015

Chairman Katko, Ranking Member Rice, and Members of the subcommittee, thank you for the opportunity to provide the views of airport operators on access control measures. As the president and CEO of Airports Council International—North America (ACI–NA), I am submitting this testimony today on behalf of the local, regional, and State governing bodies that own and operate commercial service airports in the United States and Canada. ACI–NA member airports enplane more than 95 percent of the domestic and virtually all the international airline passenger and cargo traffic in North America. More than 380 aviation-related businesses are also members of ACI–NA.

Mr. Chairman, each day, airports, operating in today's dynamic threat environment, implement a variety of measures to provide for the security of their passengers, employees, and facilities. To this end, airports partner with the Transportation Security Administration (TSA), U.S. Customs and Border Protection (CBP), the Federal Bureau of Investigation (FBI), other Federal, State, and local law enforcement agencies, and airlines to develop and maintain a comprehensive, multilayered, risk-based aviation security system. In our testimony, we have included several recommendations to enhance airport access control.

LAYERS OF SECURITY

Airport access control systems rely on multiple risk-based layers of security implemented in partnership with airports, airlines, and the TSA. Although there is no perfect security system, the multiple layers—which are routinely enhanced—provide for the security of passengers, employees, and facilities. A clear strength of this type of system is the unpredictable nature of the individual layers of security and the fact that many airports go above and beyond the baseline security requirements, implementing additional processes, procedures, and technologies that take account of and are adapted to their unique geographic locations and facility designs.

This system—in combination with TSA's employee-focused security initiatives—is more effective than a rigid, fixed-point 100 percent employee screening regime that would be extraordinarily costly, minimally reduce risk and significantly disrupt airport operations. In accordance with the current system, employees are subject to search, inspection, or screening at any point, not just when they enter through an access control point. Therefore, the current system more effectively mitigates risk through employees' expectation of being screened at any point and by accounting for employees found to be in possession of items—necessary in the performance of their assigned duties—that would otherwise be considered prohibited.

EMPLOYEE BACKGROUND SCREENING

An essential layer of security is the multi-faceted employee background screening process which is initiated prior to an employee being granted access to the secured area of an airport. In advance of issuing a Security Identification Display Area (SIDA) badge, which provides unescorted access to secure areas, airport operators conduct extensive vetting of employee backgrounds. There are two critical facets of the employee background screening regime that all employees who work in secured areas must successfully pass: A fingerprint-based Criminal History Records Check (CHRC), and a Security Threat Assessment (STA). Upon receiving an application from an employee seeking unescorted access to a secured area, airport operators validate the identity of the individual, collect and transmit their fingerprints and the associated biographic information to the TSA. The biometric fingerprint data is routed by TSA to the FBI for a CHRC. Through the STA process, TSA conducts a threat assessment against terrorism and other Government databases.

If the STA reveals derogatory information about the individual, TSA informs the airport operator that they must not issue a SIDA badge granting unescorted access. If at any point thereafter recurrent STA vetting reveals derogatory information about an employee with unescorted access, TSA will notify the airport operator to immediately revoke their SIDA badge. Similarly, in accordance with existing regulations, when an airport operator discovers, during a review of CHRC results, that an applicant has been convicted of a disqualifying criminal offense within the previous 10 years from the date of application ("look-back period"), they refuse to issue the individual a SIDA badge. A distinct security feature is the ability for airport operators to review each and every applicant's criminal record to make a determination about their suitability for being granted unescorted access privileges.

Furthermore, CBP regulations stipulate that only those employees with a CBP seal on their airport-issued SIDA badge may have unescorted access to the "Customs security area," commonly known as the Federal Inspection Services (FIS) area, as well as to locations where international flights deplane. In order to obtain a CBP seal, applicants must submit to a background check, which typically involves either a review of the CHRC results obtained by the airport operator in accordance with TSA regulations or through a completely separate submittal of the applicant's fingerprints and associated information for a Criminal History Investigation, as required by the CBP port director. Notably, CBP regulations contain a more extensive list of disqualifying offenses, and a requirement for denial of a CBP seal if there is "evidence of a pending or past investigation establishing probable cause to believe that the applicant has engaged in any conduct which relates to, or which could lead to a conviction for, a disqualifying offense." Given the disparity between the two lists of disqualifying offenses (TSA and CBP), there are cases in which employees have been—in accordance with regulations—granted unescorted access to the SIDA but denied a CBP seal.

Although some airports go above and beyond the baseline measures in current TSA regulations and have implemented longer "look-back periods" and an expanded list of disqualifying criminal offenses, others are unable to do so due to restrictive State laws. While some airport operators re-submit a portion of the population of SIDA-badged employees for a CHRC, it only provides a snapshot of their criminal record as of the date of submission.

EMPLOYEE TRAINING

Provided an applicant for unescorted access privileges has a clean background, but prior to being issued a SIDA badge, they must successfully complete an initial training program. This mandatory training, specifically tailored to the airport, includes information about the layers of security at the airport, the specific responsibilities of individuals who have been granted unescorted access privileges, and their obligation to support and uphold airport security requirements. In order to maintain their unescorted access privileges, employees must also participate in recurrent training.

ACCESS CONTROL SYSTEMS

Access control systems involve multiple layers of integrated processes, procedures, and technologies to detect and mitigate breaches. Although perimeter fencing and controlled access gates are the most outwardly visible features, numerous other systems, both conspicuous and inconspicuous, are in place at airports to bolster access control security. Vehicles and equipment seeking access to these areas are inspected by local law enforcement or specially-trained public safety personnel. In addition to routine patrols in secured and other airport areas, airport operators conduct random checks of employees at various access points.

Access control systems have been in place for many years at airports and vary in their level of sophistication from passive to fully automated systems utilizing active technology. Many access control systems are enhanced through the use of closed-circuit television which allows critical areas or access points to be remotely monitored. In the event of a potential breach, active systems immediately identify the location, allowing operations center representatives to assess the situation and dispatch law enforcement or other resources to protect employees, aircraft, and facilities.

The National Safe Skies Alliance, in partnership with airports, and funded through the Airport Improvement Program (AIP), conducts testing and operational evaluations of security technologies designed to further enhance access control. Many airports have deployed the systems tested and evaluated by the National Safe Skies Alliance. The reports, which are available to all airports, provide specific details about the application and functionality of technologies tested under the program and contain incredibly valuable information for airports as they make decisions on which technologies may work best at their facility.

ACI–NA member airports are committed to ensuring effective security and continue to implement measures that further augment access control. Airport operators, in coordination with the FBI, Federal, State, and local law enforcement representatives, and TSA routinely conduct risk and vulnerability assessments to identify potential weaknesses and guide the application of resources to further enhance access control procedures and technology.

RANDOM AND UNPREDICTABLE SCREENING

Another important layer of security, The Aviation Direct Access Screening Program (ADASP), a TSA initiative that utilizes roving teams of TSA Transportation Security Officers (TSOs), Behavior Detection Officers (BDOs) and Transportation Security Inspectors (TSIs) to conduct random and unpredictable physical screening of employees working in or accessing secured areas, has proven to be very effective in mitigating risk. Some airports work in close partnership with TSA in support of ADASP operations to close certain access points and funnel employees through the screening locations. Others have taken the initiative to revoke the SIDA badge of any employee who refuses to be screened during ADASP operations. The ADASP program also effectively mitigates the risk of prohibited items introduced at the perimeter, which would go undetected under a fixed-point employee screening system. In addition to introducing a high level of deterrence, this type of random and unpredictable screening program represents another formidable layer of security.

RECOMMENDED SECURITY ENHANCEMENTS

Security Awareness Training and Incentive Programs

So that airports operators are able to more effectively educate employees and tenants, and in order to leverage the benefits of enhanced airport employee awareness, TSA and the FBI should provide airport operators with the key indicators of suspicious activity, elements of which could be drawn from BDO training. With this information, airport operators could incorporate more precisely-focused security awareness training into existing SIDA initial, recurrent, and other training programs. This would ensure that all employees and tenants are more effectively trained in security awareness. In addition to providing information on identifying suspicious activity, a key element of the training would focus on reporting. Building on the success of "community policing" initiatives such as The Rewards for Justice Program and Crime Stoppers USA, a Nationally-managed incentive program should be established to further encourage the reporting of any potential suspicious or criminal activity at airports.

Enhanced Background Checks

In order to further strengthen the layer of security involving background checks, consideration should be given to expanding the list of disqualifying criminal offenses beyond those contained in current TSA regulations. The Aviation Security Advisory Committee (ASAC) should be tasked to reevaluate the current list and develop an expanded list of pertinent disqualifying criminal offenses. Furthermore, the ASAC should evaluate whether permanently disqualifying criminal offenses would enhance the integrity of the aviation security system.

We recommend that steps be taken to immediately implement the FBI's Rap Back program so that real-time recurrent CHRCs are conducted on SIDA badge holders. In accordance with existing regulations, "Each individual with unescorted access authority who has a disqualifying criminal offense must report the offense to the airport operator and surrender the SIDA access medium to the issuer within 24 hours of the conviction or the finding of not guilty by reason of insanity." Essentially, employees who, as a result of having been subjected to a stringent background check process, have been granted unescorted access privileges are on the "honor system" to report subsequent convictions for disqualifying criminal offenses. Unlike the STA process, through which TSA conducts perpetual vetting of employees who have been granted unescorted access privileges, the CHRC is currently a one-time snapshot of the applicants' criminal history. According to the FBI, Rap Back provides "the ability to receive on-going status notifications of any criminal history reported on individuals holding positions of trust." When implemented, this program will provide airports (and airlines) much better and needed visibility into employees' criminal records, allow them to make informed determinations as to the suitability of existing employees and greatly assist in making determinations about whether employees should be allowed to retain their unescorted SIDA access privileges.

Given the transitory nature of aviation workers, a National database—maintained by TSA but available to all airport operators—of employees who have had their SIDA badges revoked would provide yet another security enhancement. Such a database would eliminate the potential for an employee whose unescorted access privileges were revoked at one airport from transferring to another airport and being granted unescorted access privileges.

Expanded Employee Screening Operations

As a means to enhance an important layer of security, TSA should expand the Aviation Direct Access Screening Program (ADASP) so that every employee entering or working in a secured area of an airport has the expectation that they will be subject to screening. Airport operators can support expanded ADASP operations by selectively closing access portals in order to route employees through the screening locations.

CONCLUSION

ACI–NA and its member airports are committed to working with Congress, TSA, FBI, CBP, and other law enforcement agencies and aviation stakeholders to enhance airport security through the application of risk-based measures. The current multi-layered, risk-based aviation security system continues to be effective, particularly as airport operators—in partnership with TSA—routinely review security procedures to ensure they are applicable and mitigate new and emerging threats.

We encourage the subcommittee to make it a priority to move forward with the implementation of the recommended initiatives to enhance airport security. Through continued collaboration to enhance security programs and related security initiatives, we can better achieve our mutual goals of enhancing security and efficiency while minimizing unnecessary operational impacts.

Thank you for the opportunity to submit this written testimony.

LETTER FROM THE AMERICAN ASSOCIATION OF AIRPORT EXECUTIVES

FEBRUARY 2, 2015.

The Honorable JOHN KATKO,
Chairman, Subcommittee on Transportation Security, Committee on Homeland Security, U.S. House of Representatives, Washington, DC 20515.

The Honorable KATHLEEN RICE,
Ranking Member, Subcommittee on Transportation Security, Committee on Homeland Security, U.S. House of Representatives, Washington, DC 20515.

DEAR CHAIRMAN KATKO AND RANKING MEMBER RICE: On behalf of the American Association of Airport Executives (AAAE) and the thousands of men and women across the country who manage and operate our Nation's airports, we appreciate your interest in undertaking "A Review of Access Control Measures at Our Nation's Airports" as part of this week's hearing. A key component of an intelligence driven risk-based approach to aviation security is the constant evaluation of existing security measures to ensure any potential vulnerabilities are addressed and mitigated with appropriate and up-to-date policies, procedures and best practices at the federal and local levels.

As employees of local, public entities, airport executives work in constant collaboration with the Transportation Security Administration to enhance the layers of security that exist to identify and address potential threats in the airport environment, including extensive background checks for aviation workers, random physical screening of workers at airports, surveillance, law enforcement patrols, robust security training, and the institution of challenge procedures among airport workers.

In particular, airport access control is an important security function that local airport operators have held for decades in compliance with robust federal requirements. The existing local/federal partnership approach ensures a critical level of local involvement with the management of credentialing and access control in accordance with strict federal standards, requirements, and oversight as part of a multi-layered security apparatus. It includes extensive efforts to identify "bad" people before they are ever given access to security sensitive areas of airports, which is absolutely essential to providing the highest levels of security.

In our view, the best approach to enhancing access control at the nation's airports lies with continuing to focus on robust background checks, maintaining our multi-layered security approach, and preserving and protecting the critical local layer of security that airports provide with credentialing, access control, and other local functions. Inherently local security functions should remain local with federal oversight and backed by federal resources when appropriate.

While some have argued for comprehensive physical screening of all persons entering an airport, including employees, it is critical from a security and resource perspective that risk mitigation efforts remain intelligence driven, balanced and effective. Detailed studies by both government and industry have shown that physical screening of all employees at airports around the country would cost upwards of $15 billion annually with very little security benefit. In a world of limited resources, we are concerned that placing so much emphasis on one approach—in this case physical screening—could divert significant funding from other critical security functions that are currently producing significant benefits. We would welcome the opportunity to have a more thorough conversation with you on this topic to outline our significant reservations in more detail.

AAAE staff and several of our airport members, including the Chair of our Transportation Security Services Committee Jeanne Olivier, A.A.E., Director of Aviation Security at the Port Authority of New York and New Jersey; are serving on the ad hoc working group formed by the Aviation Security Advisory Committee (ASAC) at the request of TSA to evaluate the aviation industry's current approach to airport employee screening. The Working Group has been tasked with developing a report to TSA on current and innovative methods for the vetting and physical screening of individuals entering the secure area of an airport. It is expected that the report will outline potential security gaps or vulnerabilities and include recommendations for proposed appropriate mitigation measures and notional methods for implementation, address the advantages and disadvantages of such measures, and the potential cost of each measure.

Access control at airports is unique among other transportation facilities and has operated successfully for decades. That is not to say that improvements to the current system cannot be made. Airport operators take their direct responsibility for credentialing and access control very seriously and are committed to continuing to provide the robust layer of security and operational expertise that exists at the local level. We look forward to working through the ASAC ad hoc working group and with the TSA and the Subcommittee on identifying and implementing any risk-based options related to improving airport access control, including policy and procedures, industry best practices, technology, and employee training.

Thank you for your time and attention to this important element of security at our nation's airports. We look forward to working with the Subcommittee as you continue to undertake efforts to enhance transportation security across the country.

Sincerely,

JOEL D. BACON,
Executive Vice President, Government and Public Affairs,
American Association of Airport Executives.

Mr. KATKO. The Chairman now recognizes a second panel.

I thank both Ms. Pinkerton and Mr. Southwell for being here today. We are pleased to have this panel of distinguished witnesses, of course.

Let me remind the witness that their entire written statements will appear in the record.

Our first witness, Mr. Miguel Southwell, is general manager at Hartswell-Jackson—excuse me—Hartsfield-Jackson International Airport in Atlanta. Mr. Southwell has been the aviation general manager at Atlanta since May 2014 and has served as senior airport leadership at both Atlanta and Miami International Airports throughout his career.

The Chairman now recognizes Mr. Southwell to testify.

STATEMENT OF MIGUEL SOUTHWELL, GENERAL MANAGER, HARTSFIELD-JACKSON ATLANTA INTERNATIONAL AIRPORT

Mr. SOUTHWELL. Chairman Katko, Ranking Member Thompson, Ranking Member Rice, Members of the subcommittee, and visiting Congressman Johnson, I thank you for holding this hearing, and I thank you for including Hartsfield-Jackson Atlanta International Airport, the world's busiest passenger airport.

I want to begin my remarks with the following statement: The safety and security of airport users is our top priority. I am reassured by the remarks offered by the witnesses on the first panel. I agree that ensuring the safety and security of our passengers and employees is a crucial and collective goal for all of us.

Further, I am pleased to know that a number of the committee Members have backgrounds as prosecutors, evidencing a lifetime commitment to the safety of our Nation.

At Hartsfield-Jackson, we have had some recent incidents in the area of security which should give us all concern. There is no mistaking that fact. As the general manager for the Department of Aviation, it is my job to provide leadership to ensure that working with the Transportation Security Administration, airlines, and stakeholders, security gaps are closed, and the passengers and employees at the airport are safe. Each year we have more than 94 million passengers who pass through Atlanta. In addition, we have more than 63,000 employees on campus. Ensuring their safety and security is a big job, but I know that our partners, particularly the TSA and the airlines, are equally committed to this task.

As you know, every airport is different. Each is unique in its configuration, and each is unique in terms of its risk profile. As such, there is no one-size-fits-all approach to airport security. As with every airport in the country, we work tirelessly with our security partners and operate on the TSA-approved security plan. This multi-layered system of security measures is based upon the determined risk at a particular airport. However, we recognize that air transportation is a system, and any system is only as strong as its weakest link.

Approximately 64 million of the 94 million passengers who pass through Atlanta annually are connecting from another airport. Therefore, we believe that some minimum standard of employee screening or inspection should be adopted across the entire system and should incorporate the input of all of our U.S. airports as well as our airline partners.

As noted earlier, at our airport, we need to do more. Hence, in the last 6 weeks, the Aviation Department has held many meetings almost daily with TSA, Customs and Border Protection, the FAA, airlines, and other key stakeholders to develop an improved short-, medium-, and long-term safety and security plan for Hartsfield-Jackson Atlanta International Airport.

In our early assessments, we have identified security enhancements that can be made now while we continue to develop other security options that will take some time. I have instructed our team that we will not wait to take action. We have and will implement immediately what can be done now while we continue to improve our plan.

At Hartsfield-Jackson, one action that we can implement immediately is the reprogramming of Security Identification Display Area badges, known as SIDA badges. These are the badges which currently allow employees access to the sterile areas of the airport. This reprogramming will be based on employee job function and work location, and will effectively reduce the number of access portals through which an employee can enter the airport's secure areas.

We recognize that 100 percent screening of airport employees has operational and cost challenges, and is neither practical nor sustainable, but the unmistakable fact, as recent events suggest, is that we need to be consistently vigilant in our efforts, and the kind of enhancements that we are considering will require a significant investment.

Therefore, in the medium to long term, Atlanta will work closely with TSA, the airlines, and other key stakeholders to screen airport employees who access the SIDA. The few exceptions will include law enforcement, emergency personnel, other first responders, and those employees approved under the Federal regulation such as the TSA's Known Crew Member Program. Even with those exceptions, we have begun processes whereby all employees at Hartsfield-Jackson will have an expectation that they will be screened or inspected.

Additionally, we are focusing on improvements to employee background checks and screening. We will focus on smarter access control as noted. We are likewise focusing on the security and safety of goods brought onto the airport property. While we attempt with our partners in the security and intelligence fields to prevent individuals with ill will from working at the airport, we are also focusing on eliminating illicit materials from ever entering the airport campus.

In closing, the conversation is bigger than Hartsfield-Jackson. Passengers will not fly if they cannot take their safety for granted. Therefore, a safe and secure air transportation system also means an economically healthy system and directly impacts the entire U.S. economy. In order to achieve these security enhancements, we will need the cooperation of our partners at the airport and, in particular, the financial support and resources of the TSA. Our commitment to ensuring the safety and security of everyone at Hartsfield-Jackson is unwavering. We are up to the task, and I am confident that our partners are as well.

Thank you very much, and I look forward to your questions.

[The prepared statement of Mr. Southwell follows:]

Prepared Statement of Miguel Southwell

February 3, 2015

Chairman McCaul, Ranking Member Thompson, Chairman Katko, Ranking Member Rice, and Members of the subcommittee, I thank you for holding this hearing, and I thank you for including Hartsfield-Jackson Atlanta International Airport, the world's busiest passenger airport.

I want to begin my remarks with the following statement: The safety and security of airport users is our top priority. I am reassured by the remarks offered by the witnesses on the first panel, and I agree that ensuring the safety and security of our passengers and employees is a crucial and collective goal for all of us. Further, I am pleased to know that a number of committee Members have backgrounds as prosecutors, evidencing a lifetime commitment to the safety of our Nation.

At Hartsfield-Jackson, we have had some recent incidents in the area of security, which should give us all concern. There is no mistaking that fact. As the general manager for the Department of Aviation, it is my job to provide leadership to ensure that—working with the Transportation Security Administration (TSA), airlines, and other stakeholders—security gaps are closed, and the passengers and employees at the airport are safe. Each year, we have more than 94 million passengers who pass through Atlanta; in addition, we have more than 63,000 employees on campus. Ensuring their safety and security is a big job, but I know that our partners, particularly TSA and the airlines, are equally committed to this task.

As you know, every airport is different. Each is unique in its configuration, and each is unique in terms of its risk profile. As such, there is no one-size-fits-all approach to airport security. As with every airport in the country, we work tirelessly with our security partners and operate under a TSA-approved security plan. This multi-layered system of security measures is based upon the determined risk at a particular airport. However, we recognize that air transportation is a system, and any system is only as strong as its weakest link. Approximately 64 million of the more than 94 million passengers who pass through Atlanta annually are connecting from another airport. Therefore, we believe that some minimum standard of employee screening or inspection should be adopted across the entire system and should incorporate the input of all U.S. airports.

As noted earlier, at our airport, we need to do more. Hence, in the last 6 weeks, the Aviation Department has held meetings almost daily, with TSA, Customs and Border Protection, the FAA, airlines and other key stakeholders, to develop an improved short-, medium-, and long-term safety and security plan for Hartsfield-Jackson Atlanta International Airport.

In our early assessment, we have identified security enhancements that can be made now, while we continue to develop other security options that will take some time. I have instructed our team that we will not wait to take action. We will implement immediately what can be done now while we continue to improve our plan. At Hartsfield-Jackson, one action that we can implement immediately is the reprogramming of Security Identification Display Area badges, known as SIDA badges. These are the badges which currently allow employees access to the sterile areas of the airport. This reprogramming will be based on employee job function and work location, and will effectively reduce the number of access portals through which an employee can enter the airport's secured areas.

We recognize that 100% screening of airport employees has operational and cost challenges, and is neither practical nor sustainable. But the unmistakable fact, as recent events suggest, is that we need to be consistently vigilant in our efforts, and the kind of enhancements that we are considering will require a significant investment.

Therefore, in the medium- to long-term, Atlanta will work closely with TSA, the airlines and other key stakeholders, to screen airport employees who access the SIDA. The few exceptions will include law enforcement, emergency personnel, other first responders and those employees approved under Federal regulations such as the TSA's Known Crew Member program. Even with those exceptions, we have begun processes whereby all employees at Hartsfield-Jackson have an expectation that they will be screened or inspected.

Additionally, we are focusing on improvements to employee background checks and screening. We will focus on smarter access control as noted. We are likewise focusing on the security and safety of goods brought onto airport property. While we attempt, with our partners in the security and intelligence fields, to prevent individuals with ill will from working at the airport, we are also focusing on eliminating illicit materials from ever entering the airport campus.

In closing, this conversation is bigger than Hartsfield-Jackson. A safe and secure air transportation system also means an economically healthy system and directly impacts the entire U.S. economy. In order to achieve these security enhancements, we will need the cooperation of our partners at the airport, and in particular, the financial support and resources of the TSA. Our commitment to ensuring the safety and security of everyone at Hartsfield-Jackson is unwavering. We are up to the task, and I am confident our partners are as well.

Thank you.

Mr. KATKO. Thank you, Mr. Southwell. I appreciate it, and I appreciate you meeting with our office yesterday as well in advance of this hearing today.

Our second witness, Ms. Sharon Pinkerton, currently serves as a senior vice president for legislative and regulatory policy at Airlines for America.

Airlines for America is a trade organization of the principal U.S. airlines representing the collective interest of airlines and their affiliates who transport more than 90 percent of U.S. airline passenger and cargo traffic.

The Chairman now recognizes Ms. Pinkerton to testify. Thank you.

STATEMENT OF SHARON L. PINKERTON, SENIOR VICE PRESIDENT, LEGISLATIVE AND REGULATORY POLICY, AIRLINES FOR AMERICA

Ms. PINKERTON. Chairman Katko, Ranking Member Rice, and Members of the subcommittee, thank you for holding this hearing. The subcommittee's focus on this issue is both timely and beneficial. There is nothing more important to the airline industry than the safety and security of our passengers, employees, planes, and cargo. Our job, when it comes to safety and security, is never done. We work every day to ensure that we are as secure as we can be.

The airline industry regards recent breaches of the civil aviation security system as unacceptable. Such breaches need to be carefully examined, root causes identified, and appropriate corrective actions formulated and then implemented. Our members have started to do that, and I am going to highlight several possible initiatives concerning employee background checks and airport access practices that we believe should be considered.

The safety and security of commercial aviation is a shared responsibility, and as such, consideration should be collaborative, involving not only Government in its regulatory role but also considering the perspective of airline, airport, vendors, and employee representatives.

Despite the recent well-publicized issues, the U.S. aviation system—security system is strong and getting stronger. It is a sophisticated system that anticipates emerging threats. Its success can be attributed in large measure to the methodical application of a risk-based approach to security. It is based on the realization that one size does not fit all.

Risk-based security ranks risk factors along a quantitative scale. Once risk levels are determined, security resources are then apply in proportion to the assessed risk. It is simple and intuitive. Issues or people that exhibit higher risk and have higher risk factors receive greater scrutiny. This approach is working.

The TSA screens almost 2 million passengers daily using risk-based procedures that have greatly facilitated its multi-layered security system.

One such layer is the employee background checks of employees who have unescorted access to secured areas of U.S. airports. Access is only approved if the employee does not have a disqualifying criminal history. There is a basic record check requirement and separate background check requirements that the U.S. Customs and the Postal Service also impose. My written testimony provides more detail on those checks.

In addition to the criminal history record check programs TSA regulations require that airlines conduct daily watch list vetting for all their employees. This is an internal and automated process that matches names against the Federal watch list.

Additionally, TSA conducts random searches of employees who have access to secured areas of the airport. Moreover, it conducts a security threat assessment of those whose have airport-approved or airport-issued IDs. The assessment includes checks against criminal history records, watch lists, and immigration databases. As a partner in safety and security, we believe that the Aviation Security Advisory Committee, the ASAC, is the right venue to conduct an evaluation of where we are today and potential next steps. ASAC's mission has been to examine areas of civil aviation security with the aim of developing recommendations for improvement.

I provided more suggestions in my written testimony, but will call to your attention a few issues we believe the ASAC should look at carefully. On employee screening, we suggest expanding random screening of employees to include, for example, different airport access control entrances and company employee parking lots. In the area of background checks, ASAC should consider expanding the category of disqualifying crimes and modifying eligibility requirements for employment.

Second, we think they should consider Federal standardization of disqualifying crimes.

Third, having Federal Government-specified permanent disqualifying crimes.

Fourth, lengthening the look-back period for criminal history record checks. To that last point, the FBI's initial criminal arrest history record check, as you heard on the first panel, is based on a fingerprint, but it is only conducted at the time of employment. It has a 10-year look-back. Furthermore, there is no on-going vetting after the initial review and no current system to inform employers should an employee be charged with a crime after the criminal history record check. We believe this warrants improvement.

In closing, we have the safest and most secure commercial aviation system in the world, and we are making—we are working to make it better every day. We have gotten to this point by focusing our time and resources on our greatest risks. We also do not believe that increased security and smoothly moving passengers and employees through screening are mutually exclusive. Two of the greater wins for passengers and customers are the Known Crewmember and PreCheck programs. These programs recognize those who present a lower risk, free up space in lines, improve passenger and employee throughput, all while enhancing security. That is a win for everyone and an idea we should build on.

Thank you, and I look forward to your questions.

[The prepared statement of Ms. Pinkerton follows:]

Prepared Statement of Sharon L. Pinkerton

February 3, 2015

Airlines for America appreciates the opportunity to express its views about the security measures for employees who are authorized access to secured areas of U.S. airports.

As we discuss more fully below, our members have examined this matter in detail and have identified airport security and employee background check improvements that they believe should be considered. Those include tighter controls over employee access to airport Secured Identification Areas; better communication among law enforcement agencies about investigations of employees who have access to the airport; expansion and harmonization among Federal agencies of the crimes that disqualify a person from unescorted access at airports; enhanced risk-based screening of employees; and strengthened employee criminal history record checks.

We believe that the Transportation Security Administration's Aviation Security Advisory Committee is the appropriate venue in which to examine these matters—and any others that may be raised. The ASAC has representatives from a broad spectrum of aviation stakeholders and is the traditional site in which to develop collaboratively proposals to submit for improvements in civil aviation security.

OVERVIEW

The subcommittee's focus on this issue is both timely and beneficial.

The airline industry regards any breach of civil aviation security as unacceptable. Such breaches need to be carefully examined, root causes identified, and appropriate corrective actions formulated and implemented.

Our members have taken a fresh look at airport security. Below we highlight several possible initiatives concerning employee background checks and airport access practices that we believe should be considered. As noted above, that consideration should be undertaken collaboratively—involving not only the Government in its regulatory role but also taking into account the perspectives of airline, airport, vendor, and employee representatives.

It is important to provide context to this hearing. The recent security breaches are absolutely unacceptable. That does not change the underlying fact that the aviation security system in our Nation is more robust than ever. It is a sophisticated, threat-based system that continues to advance in anticipation of existing and emerging threats. Its success can be attributed in large measure to the methodical application of a risk-based approach to security.

The risk-based security system under which airlines and airports operate has markedly improved security. It is based on the fundamental recognition that sound security policy need not apply the same measures to every individual or item. In other words, one size does not fit all. That recognition is founded on the understanding that not every individual or item poses the same threat to aviation security.

Risk-based security ranks an array of risk factors along a quantitative scale. Once risk levels are determined, security resources are applied in proportion to the assessed risk. In operation, this means that the aviation security system deploys its resources based on individualized assessments of risk of persons (and items) that are subject to the system. Those persons determined to exhibit higher-risk factors receive greater scrutiny. This approach enables us to put resources where they are most needed.

Risk-based security in aviation has been a reality for some time. We thus have considerable, everyday experience with it. For example, the Transportation Security Administration screens about 1.8 million passengers daily using risk-based procedures. We understand risk-based security and we know its effectiveness. We consequently strongly support it. Whatever new measures may emerge concerning airport security, we firmly believe that the commitment of the Government and industry to risk-based security must remain undiminished.

Moreover, risk-based security has greatly facilitated TSA's multi-layered security system. As TSA has stated, each layer serves as a protection measure. In combination, these layers create a much stronger, better-protected transportation system. That, as experience demonstrates, is the optimum way to confront ever-evolving threats to aviation.

FEDERAL BACKGROUND CHECK REQUIREMENTS FOR AIRLINE EMPLOYEES

Background checks of employees who have unescorted access to secured areas of U.S. airports have been required since 1985. Approval for access to those areas is authorized only if the results of the check indicate that the employee does not have a disqualifying criminal history. There is a basic record-check requirement and separate background check requirements that U.S. Customs and Border Protection and the U.S. Postal Service impose. These distinct requirements are summarized below.

Criminal History Records Check

To ensure that certain designated areas of the airport have controlled access, Secured Identification Areas (SIDA) were established. These are areas on an airport in which only employees who are approved and who have received an airport-issued badge are permitted unescorted access.

A Criminal History Records Check (CHRC) is conducted to determine if an employee should be issued a SIDA badge. The employee seeking such SIDA access must be fingerprinted. Fingerprints are sent to the Federal Bureau of Investigation, which processes them.

The CHRC regulation includes a list of disqualifying crimes that originated in Federal legislation. If an employee has a conviction for any of the disqualifying crimes within the last 10 years, he or she will not be approved. If no disqualifying crimes are found in the FBI check, the airport operator notifies the authorizing employer or airline (or other sponsor) that the employee is eligible for a SIDA badge. The employee then goes to a SIDA class to learn the requirements and limitations of access to the SIDA and, upon successfully completing the class, receives an airport-issued ID badge.

U.S. Customs and Border Protection Checks

Employees working at airports where there is international service who need unescorted access to a U.S. Customs and Border Protection-designated security area must receive a CBP-issued seal for her or his identification media. To receive the seal, the employee must meet the qualifications for approval under the CHRC program and not have been convicted of any of 10 additional disqualifying crimes. In addition, CBP may deny an individual a seal if it deems her or him a risk to the public health, interest, or safety; National security; or aviation safety. Issuance of a seal also requires a certification by the employer that a "meaningful" background investigation has been conducted and that it has a need for this employee to access the CBP security area.

U.S. Postal Service Checks

Employees who have access to U.S. mail must be approved by a third and separate process. This process is not set forth by law or Federal regulation but, rather, through the contractual obligation that the USPS includes in the agreements it has with air carriers to transport mail. The employee must be fingerprinted and the fingerprints are sent to the USPS for review and approval or denial. Virtually any felony conviction within the past 10 years will result in a denial of access to U.S. mail. In addition, the Postal Service's requirements also include a negative drug test, a separate criminal history check, and legal documentation that the individual has the right to work in the United States.

Airline Vetting

In addition to these criminal history record check programs, TSA regulations require airlines to conduct daily watch list (terrorist database) vetting for all their employees. This is an internal automated process that matches names against the Federal watch list that is provided daily.

Additional TSA Actions

Beyond the above-mentioned records checks and vetting, TSA conducts random searches of employees who have access to secured areas of the airport. Moreover, it conducts a Security Threat Assessment of persons who have airport-approved or airport-issued personnel identification media. The assessment includes checks against criminal history records, terrorist watch lists, and immigration status.

ADDITIONAL SECURITY MEASURES TO CONSIDER

We believe that the Aviation Security Advisory Committee should evaluate any new airport security measures. ASAC's mission is to examine areas of civil aviation security with the aim of developing recommendations for the improvement of civil aviation security methods, equipment, and procedures. The consideration of the additional measures that we suggest would fit without difficulty within the ASAC charter. Moreover, the members of are well-equipped to perform this examination and represent a cross-section of the airport community. After the ASAC completes its examination, it would forward any recommendations that it developed to the TSA for its action.

These are the areas that we have concluded that the ASAC should examine:

Airports

1. Consider tighter controls over SIDA access control areas based on duty/higher-risk times.
2. Consider requiring that local law enforcement agencies notify Federal law enforcement agencies, i.e. the FBI and DHS, of any on-going criminal investigation of an airport employee.

Security Threat Assessments

1. Consider expanding the category of disqualifying crimes and modifying eligibility requirements for employment.
2. Consider expanding current databases that TSA searches.
3. Consider Federal standardization of disqualifying crimes.
4. Consider having the Federal Government specify "permanent disqualifying crimes." Such crimes, regardless of when they were committed, would prohibit a person from obtaining an airport SIDA badge or aviation employment in a position where he or she would have access to a sensitive security work area.

Employee Screening

1. Consider expanding random screening of employees to include, for example, airport access control entrances and company employee parking lots.
2. Consider developing a program to identify high- and low-risk airport community employees.
   a. Those employees identified as low-risk would be subjected to a risk-based screening approach.
   b. Higher-risk employees would undergo random screening more frequently, based on risk and location.

Criminal History Records Checks

The FBI's initial criminal history records check/fingerprint check is only conducted at the time of employment. It has a 10-year "look-back". There is no on-going vetting after the initial review. The industry is unable under the existing system to perform updated or random checks without again collecting fingerprints from the employee and performing a new CHRC. In view of this situation, we suggest that:

1. Consideration be given to enabling airports and airlines to perform random/specific CHRC without recollecting fingerprints in the event that suspicious activities are observed.
2. Consideration be given to lengthening the "look-back" period for criminal history checks—e.g., 18–20 years.

Furthermore, there is no current system to inform employers should an employee be charged with a crime after the criminal history records check.

1. For example, if an employee hired in Virginia is arrested in Nevada, the employer would only know of the arrest if the employee self-disclosed the arrest.
2. Consideration should be given to having the FBI conduct recurrent criminal history record checks and notification be provided to the airport/airline and/or other law-enforcement agency for follow up.

Airlines

As mentioned above, TSA requires airlines to conduct daily watch list (terrorist database) vetting of all employees. That process can be made more efficient.

1. Consideration should be given to the TSA creating a web portal whereby employers can examine new-hire employees.
   a. Employers could populate the web site with complete employee lists for perpetual vetting against the watch list.
   b. Watch list vetting of employees would then shifted from the industry to TSA responsibility, which would be a more sensible allocation of this responsibility.

This is not an exhaustive list. Other possible initiatives can be added to it.

We believe that the foregoing response would be the most advantageous way to examine potential changes to criminal history record check, vetting, and airport access measures. It would assure broad-based stakeholder input by using the long-standing ASAC. Any recommendations that were forthcoming should be mindful of the risk-based framework of current aviation security. TSA, of course, would have the ultimate authority to dispose of the recommendations.

Mr. KATKO. Well, thank you, Mr. Southwell, and, Ms. Pinkerton, both for your opening statements. They are very helpful.

Ms. Pinkerton, I want to tell you that the written submission you made was very helpful because it listed a bunch of practical solutions, some of which we will touch on during the course of my questioning here for the next 5 minutes.

In fact, a technical matter, I will recognize myself for 5 minutes of questioning.

I want to start with Mr. Southwell for a moment, please, first of all to respond to one of your comments. When you said that the conversation is bigger than Atlanta, I think you are absolutely right. I don't want you to think that we are singling out Atlanta as the sole reason we are here. Atlanta simply is—happens to be in an unfortunate position of having the most recent case, but by all means, it is not an exclusive list. I think everyone here acknowledges that.

With respect to the Harvey case, which has been discussed, quick question for you, when did you first learn of it, when the investigation was under way?

Mr. SOUTHWELL. I believe it was December 15, Mr. Chairman.

Mr. KATKO. Okay. So they worked with you. When did—did you have any knowledge about when the local authorities were first aware of it?

Mr. SOUTHWELL. Well, actually, correction. We heard—I became aware of it and the airport became aware of it in terms of its specific nature on December 19. On December 15, we did receive a call, our security office, which it often does, asking for particular movements of the employee. The exact nature or context of the inquiry on December 15 was not shared. The context was shared December 19, I believe, when the employee was arrested, 19 or 20.

Mr. KATKO. Do you have any idea when the investigation by the local authorities in New York commenced?

Mr. SOUTHWELL. No. I do not, Mr. Chairman.

Mr. KATKO. Okay. Is it fair to say that you would like to have known if it was going on for a while that—what was going on in your airport?

Mr. SOUTHWELL. We certainly would have. We understand that the investigators have a certain amount of discretion in terms of widening the number of people with knowledge, but it certainly would have been helpful.

Mr. KATKO. One of the proposals that has been propounded by others is that we have some sort of a Federal requirement under the law that local authorities that are involved in aviation-related investigations, criminal investigations, must notify the FBI office immediately. Would you support such a measure?

Mr. SOUTHWELL. Absolutely, Mr. Chairman.

Mr. KATKO. Okay. Thank you.

Now, I want to switch gears for a second here to Ms. Pinkerton. As I said, your list was wonderful, and it was very helpful and very thought-provoking going forward, and I appreciate that. Just a couple of quick questions. I won't go through things that we already have, but one question—one thing I didn't notice on here, it was maybe implicit in here was reducing the number of entry points at airports for employees.

Would you support that as part of the overall enhancement of security measures for employee access?

Ms. PINKERTON. I am sure that that is something the ASAC is going to be looking at, and it does make a lot of sense.

Mr. KATKO. Okay. That was easy. All right. Thanks.

Now, with respect to the employee screening, and, again this, this is just one of many things to consider and to put on the table, but the Miami model, for lack of better term, and the Orlando model, is that all employees are screened. Now, my idea of screening is not simply walking through a metal detector. Whatever screening measures that people take into account I think are—for the local airports is fine, but basically screening all employees when they come through the door, would you support that or would you think that is fraught with problems?

Ms. PINKERTON. Well, yeah, I think that since 9/11, Mr. Chairman, we have learned a lot as we have created this multi-layered system, and really what we have learned is that one size doesn't fit all. What we have learned is the importance of conducting risk assessments and threat assessments, and I think that is, you know, how Miami developed their system and how Orlando has developed their system, but I don't necessarily think that that one size fits all 450 airports. So I think we need to look carefully to continue to work with our partners, airports, airlines, TSA, and the FBI working together to craft solutions that make sense on an airport-by-airport basis with some general standard guidelines, of course.

Mr. KATKO. Okay. Thank you.

Last question for you and then I have got a couple more for Mr. Southwell.

Would you consider expanding the disqualifying crimes for individuals that are going to get access to SIDA badges?

Ms. PINKERTON. Absolutely. That is on our list. It is something that we think that the ASAC should look carefully at, and as you know, CBP has a broader list of disqualifying crimes, and that is probably a good place to start, and then we should think about having CBP, the Post Office, and TSA perhaps all having the same list of disqualifying crimes.

Mr. KATKO. Thank you, Ms. Pinkerton.

Mr. Southwell, just for a moment, have you participated in the ASAC review that is going on Nation-wide? Have they come to you and interviewed you yet or talked to you about what is going on in Atlanta?

Mr. SOUTHWELL. They have not.

Mr. KATKO. Okay. Do you intend to make contact with that committee?

Mr. SOUTHWELL. Yes, Mr. Chairman.

Mr. KATKO. Okay. I would ask that you do so and make sure you share your thoughts with them. I think you have a wealth of experience. Speaking of which, prior to coming to Atlanta, you were in Miami. Is that correct?

Mr. SOUTHWELL. Yes, Mr. Chairman, for 12 years.

Mr. KATKO. Miami, as we now well know has taken it upon themselves to have a more rigorous review based on a serious security breach that happened even prior to 9/11. Is that correct?

Mr. SOUTHWELL. Yes, Mr. Chairman.

Mr. KATKO. Now, what if any of those aspects of the Miami model would you contemplate using in the Atlanta airport going forward?

Mr. SOUTHWELL. In advance of the, of course, advisory committee's work, Hartsfield, Atlanta, is moving towards that model in terms of what we are currently thinking and recommending.

The model that we are creating with the random inspections and not having full screening or inspection by employees speaks, really, to an employee who just wants to have gainful employment but who may be involved in various types of smuggling activities, et cetera.

With what we have seen in the last 6 months and the evolution of course of the insider threat where you have Americans being recruited, certainly greater thought has to be given to not just giving employees the expectation that they will be screened, which is what the current system does, but giving the employee a perception of certainty that they will screened, which is what the Miami and Orlando models do, and we are certainly contemplating doing that.

Mr. KATKO. Okay. Of course, no decision has been made, but that is something that is in the mix for you.

Mr. SOUTHWELL. Absolutely.

Mr. KATKO. Okay. Again, you are the world's largest airport, and you understand the task that would be at hand if you undertook such a model.

Mr. SOUTHWELL. It is as great task, but it also is a great—something that we have to contemplate because of the high profile of Atlanta as the world's busiest passenger airport and as a threat.

Mr. KATKO. Okay. Now so I can enforce my own rule of not going over too far, I am going to pass the microphone over to Miss Rice. Thank you.

Miss RICE. Thank you, Mr. Chairman.

Ms. Pinkerton, I am struck by—I mean, I think that there are some flaws that we have all spoken about and you have certainly pointed out in terms of what can be done in the initial process, in terms of doing all the checks, background checks, and I don't know if there is anyone who can answer the question as to why someone doesn't have to provide a Social Security number. That still boggles my mind why we don't ask for that information.

But the other area of concern is, what happens in the interim between hiring and separation? If you could just expound on ways that you think the TSA, airports, the FBI can be more effective at monitoring behavior of once-hired employees while they are in the employ of—while they are working because we know we can't count on self-reporting if say someone were to be arrested or and be convicted of a crime.

Ms. PINKERTON. Right. I was very pleased to hear the discussion on the first panel. That was the first time that I had heard the FBI and the TSA actually talking about what sounded like a perpetual recurring vetting with the criminal history record check. That is absolutely something that—especially if it is available, as the first panel seemed to indicate, we should definitely be relying on an automated system as opposed to self-reporting. I think that would be a huge step forward.

Miss RICE. In your capacity, what is your biggest frustration, what are the airlines' biggest frustration in terms of the day-to-day—their ability to operate in an efficient, safe way?

Ms. PINKERTON. Well, I would describe our relationship with TSA and our airport partners as being a positive and productive one. You know, I do think sometimes the media focus and attention on the latest incident sometimes clouds our ability to analyze different options thoughtfully, and that is why I am really pleased, frankly, that Congress and the administration are giving the ASAC committee, you know, 30, 60, and 90 days to come up with some really well-thought-out recommendations.

Miss RICE. So, Mr. Southwell, I don't know if you can—I hope you can answer this question. I would imagine that there was a level of upset and frustration that you personally felt and professionally at being informed at such a late date of what was going on in your own airport.

Going forward, how do we avoid that? How do we—because, to me, information is power. Right? The more information every partner has along the way, the more powerful we can be at preventing things like this from happening. So you are in a very unique position, and I am not asking you to throw anyone under the bus, because that is not what this is about. But, you know, if I were you, I would have been really angry. So what was your first reaction, and how do we avoid that from happening, because you should have been, in my opinion, a part of everything that was going on pre-arrest?

Mr. SOUTHWELL. Well, we are working, Madam Congresswoman with the TSA as well as with the FBI, the local FBI authorities. The Atlanta police department, of course, is the one who is usually notified in those instances. We are looking to increase, for example, just historically the Atlanta Police Department is notified towards the time of apprehension. If they are not, in the instances where they are not, the Atlanta police has to sign a nondisclosure agreement. Most of the times, they don't have the particular clearance to receive the information, which is something we are working with the TSA as well as the FBI at this time.

Miss RICE. What level of—if there—obviously, we need to figure out a better screening process, whether that is—whether it goes to 100 percent screening for employees in a separate area, how—and you would really be the airport that would probably bear the brunt of this the most out of any airport in this country. Is it even feasible? I mean, the things that were are talking, about Ms. Pinkerton's suggestions, things that we are asking questions about, is it feasible?

Mr. SOUTHWELL. We believe it is feasible, to the extent you talk about full screening. That is, there will be some exceptions. There is no such thing as 100 percent screening, as I stated. There is just, from a practical point of view, if someone is having a heart attack, you can't stop the EMS folks from attending to those passengers.

It is feasible. I worked in Miami for 12 years, and I have seen it work. So I know it is feasible. There is a disparity, even as we speak, regarding the passenger screening and the employee screening that we talked about earlier. The industry as a whole is looking for ways to contain costs. In the risk-based analysis, for example, that we are using with passengers where as a passenger you submit your yourself to this extra background check to qualify as a trusted traveler. Once you pass that screening, you are rewarded with not no screening, but you are rewarded by having limited screening. You don't have to take off your jacket. You don't have to take off your shoes our take out your computer out of your carry-on, but you are screened.

The employees at Atlanta's airport go through the similar background checks, and of course, they are treated a bit differently. They are currently just swiping and not being screened, and so one of—I am not subscribing that every airport would screen all of its employees. We believe, given the high profile in Atlanta, that it will be applicable.

Miss RICE. Do you have—very quickly, do you have a system in place at the airport, and forgive me if you already answered this, to track lost or stolen SIDA badges? Is there a way to ensure that people are only going where they are—in secure areas where their job and their scope of employment requires? I mean, is there any way that you can kind-of———

Mr. SOUTHWELL. We do. We do that all day through a system of dual access restrictions.

Miss RICE. And they are effective?

Mr. SOUTHWELL. Quite—quite so. You can't just simply move—simply because you can access a concourse doesn't mean that you can go down onto a ramp. We have a large number of employees who board a bus off-site at an off-site parking lot. They enter the airfield entrances and go onto the airfield. That doesn't mean that once they get onto the airfield, that they can just simply roam around. We are looking at that, however, because we talked about one key method of managing all of this cost. We have some 70 different portals at the airport. We are looking to reduce those to 10, similar to what Miami has done. So there are ways to make it feasible.

Miss RICE. Thank you both.

Thank you, Mr. Chairman.

Mr. KATKO. Thank you, Miss Rice.

Thank you, Mr. Southwell, and, Ms. Pinkerton.

Next up is Mr. Payne, the gentleman from New Jersey.

Mr. PAYNE. Thank you, Mr. Chairman.

Ms. Pinkerton, in your view, how can TSA airports, airlines, vendors, and others all work together to mitigate the insider threat?

Ms. PINKERTON. Well, I think that we are starting to do that today by having this conversation, the sharing of ideas. Again, I was very pleased to hear that the FBI and TSA have started a pilot program to do constant perpetual vetting on criminal history records, but I would say the place where we are really formalizing that collaboration is through the ASAC committee, that this subcommittee and Congress have certainly—can solidified the role of ASAC by passing that legislation. Then I think we are working together on a local basis with our airport and TSA to follow through on some of the ideas that Mr. Southwell has put on the table.

Mr. PAYNE. Thank you.

Mr. Southwell, you just mentioned, you know, how you have employees come from off airport parking lots and then bused in. Does your airport perform physical screening functions independent of those that TSA performs randomly on employees?

Mr. SOUTHWELL. We certainly do, Mr. Congressman. We have teams of people who not only perform these. It is random at the entrance points. But also throughout the day, we perform these random checks within the concourses and the various portals of the airport.

Mr. PAYNE. Well, thank you.

Mr. Chairman, in the interest of time, I will yield back.

Mr. KATKO. Thank you, Mr. Payne.

Now the Chairman now recognizes Mr. Johnson from Georgia.

Mr. JOHNSON. Thank you.

Ms. Pinkerton, you are aware of the fact that airlines have downsized the number of employees that they have to pay directly, and they have done that by farming out certain functions to contractors. Are you aware of that phenomenon?

Ms. PINKERTON. Yes. In some instances.

Mr. JOHNSON. Now your organization, Airlines for America, does not represent contractors at the airport whose employees are performing certain tasks. Is that correct?

Ms. PINKERTON. That is correct.

Mr. JOHNSON. Mr. Southwell, what percentage of that 40,000 employee number that you stated earlier are subcon—or contract employees of airlines? Because you have airline employees, you have airport employees, and you also have contractor employees at the airport. What percentage of the number are contractor employees?

Mr. SOUTHWELL. Congressman, I don't know what that number is, but I would imagine the vast majority of those employees are actually employees of the airline.

I would also like to clarify because of your question that the airlines, which represent about half of the employees on the airport that have SIDA access, actually submit all of the information to the FBI to do the background check.

Mr. JOHNSON. Well, you are kind of getting ahead of me then.

I was wanting to know whether or not these contractor employees are considered employees who are subject to these employee background checks and, also, terrorist watch list checks?

Ms. PINKERTON. Yes, Congressmen. They are.

Mr. JOHNSON. They are?

Ms. PINKERTON. They are.

Mr. JOHNSON. Well, let me ask you this, Mr. Southwell. Thank you for that response. That is comforting.

What impact has Georgia's Guns Everywhere Law, the law that allows guns to be carried in churches, in bars, in restaurants serving alcohol, in Government buildings, what impact has that law, which went into effect, I believe, in July of last year, had on airport security if any?

Mr. SOUTHWELL. Mr. Congressman, we have not seen any increase or marked increase in the number of weapons being brought to the airport. The Federal Government still has a restriction regardless of the Federal law of passengers taking guns beyond the security checkpoint.

Mr. JOHNSON. Thank you.

I would close out by saying that this morning I had the pleasure of meeting with you, Mr. Southwell, and I think we had a very thorough and productive conversation. I want to pledge to work with you to achieve the kind of security that you deem is appropriate and necessary for Atlanta Hartsfield Airport.

I want to take the liberty of, on your behalf, extending to the leadership of this committee an invitation to visit Atlanta and take a tour. When you do that, I would like to come with you and see the arrangements that are in place and that are being put in place to enhance security at the airport.

Last I would just like to say again thank you for allowing me to participate in this very important hearing today. Thank you.

Mr. KATKO. Well, I would like to thank you, Mr. Johnson.

I think we are going to take you up on that offer. I think it is important to come to Atlanta to see how things are going, and it would be very instructive for both of us.

I want to thank the witnesses for their testimony, both Mr. Southwell and Ms. Pinkerton, as well as the others. The Members of the committee may have some additional questions. As always, the hearing record will be held open for 10 days.

But I want to note that I appreciate the professionalism of both of you today as well. I mean, the one thing that is very heartening is that, instead of sweeping the problem under the rug, the industry has recognized it is a problem and we are going to work together to solve it. You know, you can rest assured you have a partner in Miss Rice and myself to do that.

Last, I want to thank Miss Rice as well. She has been a very good partner here. I look forward to working with you going forward.

So thank you.

Ms. PINKERTON. Thank you, Mr. Chairman.

Mr. KATKO. All right. Without objection, the committee stands adjourned.

Thank you.

[Whereupon, at 4:39 p.m., the subcommittee was adjourned.]

A REVIEW OF ACCESS CONTROL MEASURES AT OUR NATION'S AIRPORTS, PART II

Thursday, April 30, 2015

U.S. House of Representatives,
Subcommittee on Transportation Security,
Committee on Homeland Security,
Washington, DC.

The subcommittee met, pursuant to call, at 2:11 p.m., in Room 311, Cannon House Office Building, Hon. John Katko [Chairman of the subcommittee] presiding.

Present: Representatives Katko, Rogers, Ratcliffe, Rice, and Keating.

Mr. Katko. First of all, welcome back, Mr. Carraway. Thank you for being here again.

I would like to welcome everyone to today's hearing on airport access controls, which serves as a follow-up to the subcommittee's first hearing of the 114th Congress on this very important topic.

At the outset, I would like to express my support for President Obama's announcement of his intent to nominate Vice Admiral Peter Neffenger, current vice commandant of the U.S. Coast Guard, to be the next administrator of the TSA.

TSA provides vital security to protect our Nation's transportation systems, and it is an imperative that the agency is equipped with the necessary leadership to ensure that it is operating in the most effective and efficient manner.

I urge the Senate to act quickly on the nomination of Vice Admiral Neffenger to be TSA administrator.

A number of serious security breaches by employees at major airports in the United States in recent months has highlighted the need for the TSA, the airport stakeholder community, and this subcommittee to take a hard look at how we can work together—and I stress the word "together"—to improve access controls and employee vetting at our Nation's airports.

I hope today's hearing can provide a positive and productive dialogue on how this can be accomplished. Unlike some of the hearings, I would note parenthetically, we are going to ask your opinion on a lot of things, and we welcome your input.

In January of this year, Acting Administrator Carraway requested that the Aviation Security Advisory Committee conduct a review of airport access control measures. Today, with the final report in hand, the subcommittee intends to better understand the ASAC's findings and discuss the feasibility of the recommendations.

The ASAC report included 28 recommendations to improve airport employee access control in five general areas, including, No. 1, security screening and inspection; No. 2, vetting of employees and security threat assessments; No. 3, internal controls in auditing of airport-issued credentials; No. 4, risk-based security for higher risk populations and intelligence; and No. 5, security awareness and vigilance.

I am eager to hear how TSA and the airport community plan on improving the employee vetting process for individuals who have access to secure and sterile parts of the airport, as well as how the screening of these employees when they come to work can be improved.

In response to Acting Administrator Carraway's request, the ASAC created a working group tasked with analyzing the adequacy of existing security measures, as well as issuing recommendations on what additional measures could be implemented to improve employee access controls.

One of the initial areas the working group examined was the practicality of conducting 100 percent employee screening. Rather than 100 percent screening, the working group believes that TSA should expand random employee screening and inspection under its Playbook operations.

I am pleased that TSA has already begun increasing the random screening for aviation employees at our Nation's airports. I look forward to hearing about the methodology TSA uses to determine the frequency of conducting such screening, as well as whether that methodology is effective in providing airport employees with the expectation that they will be subject to screening while working at an airport.

Today, we have the assistant administrator of TSA, as well as two representatives from the airport community to address how those recommendations can be implemented at airports Nationwide. I applaud the efforts of the ASAC in finding ways in which access control at our Nation's airports can be further improved through the cooperation of TSA industry stakeholders.

Further, I look forward to having a meaningful discussion with TSA and airport stakeholders on what can be done going forward to improve employee vetting and screening for those with access to sensitive and sterile parts of airports.

[The statement of Chairman Katko follows:]

STATEMENT OF CHAIRMAN JOHN KATKO

APRIL 30, 2015

I would like to welcome everyone to today's hearing on airport access controls which serves as a follow-up to the subcommittee's first hearing of the 114th Congress on this very important topic.

At the outset, I would like to express my support for President Obama's announcement of his intent to nominate Vice Admiral Peter Neffenger, current vice commandant of the U.S. Coast Guard, to be the next administrator of the Transportation Security Administration. TSA provides vital security to protect our Nation's transportation systems and it is imperative that the agency is equipped with the necessary leadership to ensure that it is operating in the most effective and efficient manner. I urge the Senate to act quickly on the nomination of Vice Admiral Neffenger to be TSA administrator.

A number of serious security breaches by employees at major U.S. airports in recent months have highlighted the need for the Transportation Security Administration, the airport stakeholder community, and this subcommittee to take a hard look at how we can work together to improve access controls and employee vetting at our Nation's airports. I hope today's hearing can provide a positive and productive dialogue on how this can be accomplished.

In January of this year, Acting Administrator Carraway requested that the Aviation Security Advisory Committee conduct a review of airport access control measures. Today, with the final report in hand, the subcommittee intends to better understand the ASAC's findings and discuss the feasibility of the recommendations.

The ASAC report included 28 recommendations to improve airport employee access control in five general areas including: (1) Security screening and inspection; (2) vetting of employees and security threat assessment; (3) internal controls and auditing of airport-issued credentials; (4) risk-based security for higher-risk populations and intelligence; and (5) security awareness and vigilance.

I am eager to hear how TSA and the airport community plan on improving the employee vetting process for individuals who have access to secure and sterile parts of the airport, as well as how the screening of these employees when they come to work can be improved.

In response to Acting Administrator Carraway's request, the Aviation Security Advisory Committee created a working group tasked with analyzing the adequacy of existing security measures, as well as issuing recommendations on what additional measures could be implemented to improve employee access controls.

One of the initial areas the working group examined was the practicality of conducting 100% employee screening. Rather than 100% screening, the working group believes TSA should expand random employee screening and inspection under its playbook operations. I am pleased that TSA has already begun increasing the random screening for aviation employees at our Nation's airports. I look forward to hearing about the methodology TSA uses to determine the frequency of conducting such screening, as well as whether that methodology is effective in providing airport employees with the expectation that they will be subject to screening while working at an airport.

Today, we have the assistant administrator of TSA as well as two representatives from the airport community to address how those recommendations can be implemented at airports Nation-wide.

I applaud the efforts of the Aviation Security Advisory Committee in finding ways in which access controls at our Nation's airports can be further improved through the cooperation of TSA and industry stakeholders. Further, I look forward to having a meaningful discussion with TSA and airport stakeholders on what can be done going forward to improve employee vetting and screening for those with access to sensitive and sterile parts of airports.

Mr. KATKO. The Chairman now recognizes—well, actually, we are going to recognize Miss Rice for an opening statement, but she is not here yet. So when she gets here, we will recognize her. Other Members of the committee are reminded that opening statements may be submitted for the record.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

APRIL 30, 2015

This is the second subcommittee hearing on airport access control measures. At our first hearing on this issue in February, I stated that each airport presents a unique set of security issues. While I understand the need for vendors and airline employees to access various areas of the airport to do their jobs, I also understand the need to maintain security. That is why all airline and airport workers with unescorted access to areas beyond the checkpoint must successfully complete terrorism and criminal background checks.

At many airports, these vetted workers use their Secure Identification Display Area (SIDA) badges to bypass TSA security screening to get to their workplace—which happens to be on the other side of the TSA checkpoint. In most cases, granting vetted airport personnel such access to the sterile side of the airport is beneficial to airport operations and the flying public.

However, in December 2014, we learned of an alarming instance of SIDA badge misuse. Individuals were charged with smuggling over 150 guns from Atlanta to New York City aboard commercial flights. It seems that one of the gun smugglers used his SIDA badge to bypass physical screening to pass the weapons to a co-conspirator on the sterile side of the airport. After this incident, TSA asked the Aviation Security Advisory Committee to reevaluate airport employee screening protocols. Involving the ASAC was a good decision by Acting Administrator.

The ASAC is comprised of stakeholders within the aviation community who have a deep knowledge of the inner workings of our Nation's airports and have valuable insights to offer on how to implement security efforts in a way that does not unduly disrupt or interfere with airport operations. Last year, I was pleased that the President signed into law a measure that I authored—the "Aviation Security Stakeholder Participation Act of 2014"—to authorize this important advisory committee.

I am pleased that the ASAC acted, and in its 90-day review, set forth a number of considerations and approaches to address potential airport security vulnerabilities. The ASAC made a total of 28 recommendations. Among them was a recommendation that TSA strengthen the vetting procedures when screening employees. It also recommended that TSA maintain a database of all employees who have had credentials revoked.

For quite some time, I have often questioned TSA about its recordkeeping of lost and revoked credentials. Together with Ranking Member Rice, I have asked the Government Accountability Office to look into this. I am looking forward to learning how TSA plans on addressing this matter. The ASAC also recommended that airports limit the number of access points into sterile areas and restrict access privileges when not needed and that airports enhance auditing practices for issued badges. I look forward to hearing Mr. Grossman's perspective, as an airport official, on this recommendation as he testifies on the second panel today.

Furthermore, the ASAC recommended that TSA improve its insider threat program. While there is a case to be made for such enhancements, often with such programs, the devil is in the details. It is critical that TSA's insider threat program have strong protections to ensure that the program cannot be exploited to abuse, improperly target, or retaliate against airport workers.

I was pleased that DHS took timely action, in response to the ASAC recommendations. Within days, DHS Secretary Johnson took immediate actions to enhance aviation security. These actions include screening of airport employees when they travel as passengers and increasing randomization screenings of aviation employees.

Secretary Johnson also directed TSA to work towards requiring recurrent criminal history records checks for SIDA badge holders. While these are steps in the right direction, tough questions remain about the internal controls at our Nation's airports and whether meaningful progress can be made to address known access control vulnerabilities.

Airport security is a shared concern, and we must work across the aisle to make sure that we strike the right balance at our Nation's airports to protect the American flying public and our critical aviation infrastructure, while ensuring the free flow of commerce and people. I look forward to continued work with this subcommittee, the ASAC, and TSA to ensure the layers of security are as strong as they should be.

Mr. KATKO. We are pleased to have two very distinguished panels of witnesses before us today on this important topic. For our first panel, I would like to welcome back Acting Administrator Carraway. Let me remind the witness that his entire written statement will appear in the record.

Mr. Carraway, as we know from previous testimony, became acting administrator of TSA in January 2015. Prior to his current role, Mr. Carraway served as a deputy administrator beginning in July 2014. He has been with TSA since 2004, and has held various positions within the Offices of Security Operations and the Law Enforcement/Federal Air Marshal Service, including Supervisory Federal Air Marshal in charge for the Dallas Field Office.

The Chairman now recognizes Mr. Carraway to testify.

Mr. Carraway, welcome back, my friend.

STATEMENT OF MELVIN J. CARRAWAY, ACTING ADMINISTRATOR, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. CARRAWAY. Good afternoon, Chairman Katko, Ranking Member Rice, and distinguished Members of the committee. I appreciate the opportunity to appear before you and provide an update on TSA's efforts to mitigate the insider threat at our Nation's airports.

Controlling access to the sterile side of the airport or the area beyond the TSA's screening checkpoint requires balancing security with the business operations of each unique airport. The sterile area holds passengers and air crews waiting for flights, but it is also the workplace for vendors, mechanics, ground crews, and others employed by the airlines and the airports, many of whom enter and exit the areas multiple times a day as a part of their regular duties.

In January 2015, I asked the Aviation Security Advisory Committee, or ASAC, which we call it, to review airport access controls following the December 2014 incident in Atlanta by a Delta Airlines employee allegedly conspiring to smuggle firearms from Atlanta to New York. Following a 90-day comprehensive review, this group of industry experts delivered its report with recommendations to address vulnerabilities posed by an insider threat at our Nation's airports.

It is important to note that TSA's engagement with the ASAC on this important issue did not stop with the delivery of this report. TSA officials, including myself, have been actively engaged with our private-industry partners to ensure effective and prompt response to the recommendations provided by the ASAC.

Recognizing the potential for terrorists to exploit the vulnerability highlighted in the December 2014 events, I took several steps to address the insider threats at airports Nation-wide. These included increasing TSA random and unpredictable employee screening, reminding airlines that employees on personal travel must be screened at TSA checkpoints, and increasing communication between TSA and our aviation industry partners on threats and potential vulnerabilities.

While these actions could be initiated in the immediate short term, I also recognize the need to adopt long-term solutions. The recommendations contained in the ASAC 90-day review are comprehensive, thoughtful, and will help TSA achieve meaningful reforms and partnerships with our aviation stakeholders. Additionally, these recommendations use a risk-based approach, allowing resources to be used where they are needed the most.

The ASAC identified five areas of analysis where TSA and industry could take action to address potential vulnerabilities. These areas include security screening and inspection, employee vetting and security assessments, internal controls and auditing of airport-issued credentials, risk-based security for high-risk populations and intelligence, and security awareness and vigilance.

The ASAC generated 28 recommendations focusing on activities under TSA's jurisdictions from these five areas. Following my initial review, I found that all of these recommendations have merit. Some are achievable in the short term; however, there are many that require more thorough review to determine how to implement and if doing so will require statutory changes and/or additional resources.

Yesterday, TSA issued updates to current security directives and issued an information circular to implement the measures Secretary Johnson announced last week. They are: Requiring the fingerprint-based criminal history records check every 2 years for all airport employee SIDA badge holders until TSA establishes a system for real-time recurring criminal history background checks for all aviation workers; require airport and airline employees traveling as passengers to be screened by TSA prior to travel; requiring airports to reduce the number of access points to secured areas to an operational minimum; and increase aviation employee screening to include random screenings throughout the workday. Finally, to reemphasize and leverage the Department of Homeland Security "If You See Something, Say Something" initiative to improve situational awareness and encourage reporting suspicious activity.

Over the coming months, TSA will examine the means and ability to implement additional recommendations designed to strengthen security at our Nation's airports even more. I appreciate the ASAC's review. I look forward to continued engagement with them and our industry partners.

The ASAC also noted that requiring 100 percent physical employee screening would divert limited resources from other critical security functions and may also require infrastructure improvements, workforce expansion, and airport reconfiguration. It concluded that a random screening strategy would be the most cost-effective solution.

As noted by the 9/11 Commission, perfection is unattainable and its pursuit unsustainable. Trying to eliminate all risks results in ineffective security and unnecessarily burdens the aviation industry and Government.

Transportation security remains a shared responsibility among Government agencies, stakeholders, and aviation employees and the traveling public. I want to thank the committee for your partnership on this and other important issues, and I truly look forward to working with you and to answering your questions on this important topic.

[The prepared statement of Mr. Carraway follows:]

Prepared Statement of Melvin J. Carraway

April 30, 2015

Good afternoon Chairman Katko, Ranking Member Rice, and distinguished Members of the committee. I appreciate the opportunity to appear before you today to provide updates on the Transportation Security Administration's (TSA) efforts in enhancing airport access control at our Nation's airports.

In January 2015, I requested that the Aviation Security Advisory Committee (ASAC) convene a working group of industry experts to conduct a comprehensive review of airport access control following the December 2014 incident of a Delta airlines employee allegedly conspiring to smuggle firearms from Hartsfield-Jackson Atlanta International Airport (ATL) to John F. Kennedy International Airport in New York. The ASAC was tasked with examining the potential vulnerabilities for terrorist activities exposed by this criminal incident to determine if additional risk-based security measures, resources, or policy changes were necessary. After a 90-day comprehensive review, the ASAC delivered its report with 28 recommendations to address vulnerabilities at our Nation's airports. I would like to report on these recommendations and share with you TSA's next steps in addressing them.

ACCESS CONTROL BACKGROUND

Each day, TSA facilitates and secures the travel of nearly 2 million air passengers at approximately 440 airports Nation-wide. Controlling access to the sterile side of the airport, or the area beyond the TSA screening checkpoint, requires finding the right balance between security and the business operations of each unique airport. The sterile area hosts passengers and air crews waiting for flights, but it is also the workplace for vendors, mechanics, ground crew, and others employed by the airlines and the airports, many of whom enter and exit the area multiple times a day as part of their regular duties.

TSA requires each airport to have a security program that includes controlling access to the sterile area, and TSA inspects against these plans to ensure compliance. These inspections include checks of credentialing, perimeter security, exit lanes, employee access, and other critical areas.

EMPLOYEE VETTING AND SCREENING

TSA has established requirements for security background checks for airport and airline employees who have unescorted access to the sterile area and air operations area. This check is conducted through the Secure Identification Display Area (SIDA) badging process before employees are granted unescorted access to the sterile area of the airport. TSA conducts the name-based portion of the security threat assessment, which includes an immigration status check and recurrent checks against the Terrorist Screening Database. Additionally, under TSA regulations, airports are required to collect and submit fingerprints for a Criminal History Records Check (CHRC) and adjudicate any criminal history data for potential employees. Individuals who have committed a statutorily-defined disqualifying offense within the preceding 10 years are not eligible for a SIDA badge. While the CHRC is currently a single point-in-time check prior to employment, TSA has been working diligently towards solutions to provide recurrent vetting of the criminal history data of employees.

Once workers are employed at airports, TSA requires airports to conduct random physical inspections of employees entering restricted areas, including identification verification and checks for prohibited items. TSA also screens workers on a random and unpredictable basis as they enter restricted areas. TSA's screening protocols vary by time, location, and method to enhance unpredictability. Employees who fail to follow proper procedures in accessing secure areas may be restricted from future access, disciplined by their employer up to and including removal, or subject to criminal charges and civil penalties.

IMMEDIATE ACTIONS TAKEN BY TSA

In the immediate aftermath of the December 2014 events, I took several steps to strengthen access control security and mitigate the potential vulnerability associated with aviation workers' access to secure areas. These actions include: Increasing TSA random and unpredictable screening of airport employees as they enter for work within the sterile area; issuing letters to airlines reiterating that employees on personal travel must be screened at TSA checkpoints; and increasing communication between TSA and our aviation industry partners on threats and potential vulnerabilities.

While these actions can be conducted in the short term, I also recognized the need to adopt long-term solutions and the opportunity to engage stakeholders in the development of these solutions through consultation with the ASAC, TSA's primary advisory body comprised of industry and security representatives.

AVIATION SECURITY ADVISORY COMMITTEE REPORT

While the measures TSA has in place for background checks, security programs, and compliance inspections provide a good baseline for access control security, the December incident of alleged gun smuggling by an employee with SIDA access illustrated a need to consider additional options to address the potential vulnerability of a terrorist utilizing insider threat methods. Thanks to this committee's work in passing into law the Aviation Security Stakeholder Participation Act, codifying the ASAC's existence and strengthening its supporting role for TSA's mission, the ASAC was the ideal consultation approach to review access control vulnerabilities. The ASAC's membership of industry, law enforcement, and other key stakeholders brought a broad range of perspectives to the problem of insider threat and access control. The recommendations in their 90-day review are comprehensive, thoughtful, and will help TSA achieve meaningful reforms in partnership with our aviation stakeholders. Additionally, these recommendations use a risk-based approach, allowing resources to be used in the most efficient way for the most effective security.

The ASAC identified five areas of analysis and generated 28 recommendations in each of these areas where TSA and industry can take action to address potential vulnerabilities. These areas are:

- Security Screening and Inspection;
- Vetting of Employees and Security Threat Assessments;
- Internal Controls and Auditing of Airport-Issued Credentials;
- Risk-Based Security for Higher-Risk Populations and Intelligence; and
- Security Awareness and Vigilance.

These recommendations focus on activities under the jurisdiction of the TSA granted to it under the Aviation and Transportation Security Act (ATSA, Public Law 107–71 November 19, 2001). The ASAC expects that these recommendations will concurrently mitigate criminal activity in the secured and sterile areas of airports as well.

In terms of security screening and inspection, ASAC recommended that TSA and industry work together to increase the frequency of random and unpredictable screening for airport and airline employees. On employee vetting and security threat assessments, ASAC recommended updating the list of disqualifying criminal offenses and implementing recurrent criminal history records checks for airport and airline employees. Regarding internal controls and auditing credentials, ASAC recommended TSA and industry strengthen policies for proper airport identification media and penalties associated with credential misuse. On risk-based security, ASAC recommended TSA continue to work with our Federal intelligence partners and share intelligence information as broadly as possible and appropriate with industry partners. With respect to security awareness, ASAC recommended TSA, industry and law enforcement partners work collaboratively to share best practices and encourage employee engagement on reporting suspicious activity.

The individuals employed by airlines and airports hold positions of trust and as mentioned above are repeatedly vetted against the Terrorist Watchlist. The ASAC recognized the unique role that airline and airport workers may have, including responsibility in securing the airport environment, and recommended leveraging this workforce to its fullest potential. By creating a culture of awareness for all airport employees, through increased training and promotion of the Department of Homeland Security “If You See Something, Say Something™” program and other initiatives, these employees can serve as a force multiplier and further enhance access control measures.

As a result of ASAC’s review, on April 20, 2015 Secretary of Homeland Security Jeh Johnson announced a number of additional steps TSA will take to address the potential insider threat vulnerability at U.S. airports. First, until TSA establishes a system for real-time recurrent criminal history background checks for all aviation workers, we will require airports and airlines to conduct fingerprint-based Criminal History Records Checks every 2 years for all employee SIDA badge holders. We will reinforce existing requirements that all airport and airline employees traveling as passengers are screened by TSA prior to travel. We will direct and work with airports to reduce the number of access points to secured areas to an operational minimum. Additionally, TSA will require airports to increase aviation employee screening, to include additional randomization screening throughout the workday. Finally, we will work with our stakeholder partners to emphasize and leverage the Department of Homeland Security’s “If You See Something, Say Something™” initiative to improve situational awareness and encourage detection and reporting of threat activity.

These enhancements to access control Nation-wide will greatly improve our effectiveness by reducing vulnerabilities and maintaining our risk-based approach to aviation security. Over the coming months, TSA will examine additional recommendations to implement in the future to continue strengthening our Nation’s airports. I appreciate the ASAC’s timely and thoughtful review, and look forward to working with them and our industry partners.

Of note, the ASAC held the consensus opinion that while physical screening of employees is one means of deterring terrorist activity, 100 percent physical employee screening is not the only, or necessarily the best, solution. Requiring 100 percent physical employee screening would divert limited resources from other critical security functions. Such physical screening, moreover, would require infrastructure improvements, workforce expansion, and airport reconfiguration. This would constitute an ineffective use of resources with limited security value. An ASAC working group concluded that “the provision of so-called ‘100 percent measures’ as a layer of airport security does not appreciably increase the overall level of system-wide protection, nor does it lower over-all risk." It concluded that a random and unpredictable screening strategy would be the most cost-effective solution.

For TSA, risk-based security considers how to provide the most effective security in the most efficient way to fulfill our counterterrorism mission and protect the traveling public. As noted by the 9/11 Commission, perfection is unattainable and its pursuit unsustainable. Trying to eliminate all risk results in ineffective security and unnecessarily burdens the aviation industry and Government.

CONCLUSION

Transportation security remains a shared responsibility among Government agencies, stakeholders, aviation employees, and the traveling public. TSA will continue to apply risk-based, intelligence-driven security measures to address vulnerabilities associated with employees who have access to aircraft and secure areas of the airport, while working with industry representatives and the public to strengthen aviation security.

I want to thank the committee for your continued partnership on this and other important issues, and I look forward to answering your questions.

Mr. KATKO. Thank you, Mr. Carraway. I will note that you are remarkably on the button time-wise, which is a rarity as I am finding out on this committee.

I will note also that it is heartening to have a problem be identified by everybody and to call a hearing and for everyone to come to the table, not to fight about whether it is a problem, to acknowledge a problem, and working together to find a solution. That is how it is supposed to work, and I am glad that we are here today to work on working out—not to decide whether or not there is a problem, we are way past that—how to fix it. That is why I am glad we are here.

Mr. CARRAWAY. Yes, sir.

Mr. KATKO. The Chairman now recognizes Ranking Minority Member of the subcommittee, the gentlelady from New York, Miss Rice, who is as busy and I am, and she was a few minutes late getting here. So I want to give her an opportunity to give her opening statement.

Miss RICE. Thank you for calling me out on that, Mr. Chairman, I appreciate that. I want to thank you for convening this very important hearing.

Recent incidents, most notably the gun-smuggling operation involving a Delta employee, have highlighted the urgent need for us to look closely at access controls in our Nation's airports and the potential threat of employees exploiting security credentials to commit criminal activity, like we saw in Atlanta, or even to commit acts of terrorism.

Our first oversight hearing in February revealed what I think we would all agree to be alarming vulnerabilities that exist in regard to employee screening, employee vetting, and access controls. These vulnerabilities constitute a major threat to our homeland security and they must be eliminated.

As part of our effort to correct those deficiencies, Acting Administrator Carraway asked the Aviation Security Advisory Committee, or ASAC, to review security measures for industry employees. The ASAC, which was codified into law by legislation that Ranking Member Thompson offered last year, recently released its 90-day report on access control.

First, I want to thank the members of the advisory committee for their swift and diligent response. Obviously, we are very grateful for your work. I also want to say that I am pleased to see that the

ASAC is working exactly as it was intended. The job of maintaining our aviation security doesn't fall solely on the TSA or any one agency or entity. It is and must be a collaborative effort, and that is why this advisory committee serves such an important purpose.

The ASAC brings all the stakeholders to the table, from Federal agencies and law enforcement to leaders in the aviation industry, so that we can consider all perspectives and work together to identify ways to make our aviation system safer and more secure.

That kind of collaboration is exactly what this report represents. The 28 recommendations in the report are thoughtful, constructive, and well-researched, and I look forward to the dialogue today to understand how they can help us strengthen security procedures, tighten access controls, and neutralize the insider threat.

So, Mr. Carraway, thank you very much for your appearance, and for all of the witnesses here today. Thank you.

[The statement of Ranking Member Rice follows:]

STATEMENT OF RANKING MEMBER KATHLEEN M. RICE

APRIL 30, 2015

Recent incidents—most notably the gun-smuggling operation involving a Delta employee—have highlighted the urgent need for us to look closely at access controls in our Nation's airports and the potential threat of employees exploiting security credentials to commit criminal activity like we saw in Atlanta, or even to commit acts of terrorism.

Our first oversight hearing in February revealed alarming vulnerabilities that exist in regard to employee screening, employee vetting, and access controls. These vulnerabilities constitute a major threat to our homeland security, and they must be eliminated.

As part of our effort to correct those deficiencies, Acting Administrator Carraway asked the Aviation Security Advisory Committee, or ASAC, to review security measures for industry employees. The ASAC, which was codified into law by legislation that Ranking Member Thompson offered last year, recently released its 90-day report on access control.

First, I want to thank the members of the Advisory Committee for their swift and diligent response—we're very grateful for the work you put into this report. I also want to say I'm pleased to see the ASAC working exactly as it was intended. The job of maintaining our aviation security doesn't fall solely on the TSA, or any one agency or entity. It is and must be a collaborative effort, and that's why this advisory committee serves such an important purpose.

The ASAC brings all the stakeholders to the table—from Federal agencies and law enforcement, to leaders in the aviation industry—so that we can consider all perspectives and work together to identify ways to make our aviation system safer and more secure. That kind of collaboration is exactly what this report represents. The 28 recommendations in the report are thoughtful, constructive, and well-researched. And I look forward to the dialogue today to understand how they can help us strengthen security procedures, tighten access controls, and neutralize the insider threat.

I want to thank each of our witnesses for being here today. I thank Acting Administrator Carraway for his service, and look forward to hearing his perspective on how the TSA will work with industry partners to act on these recommendations, as well as how TSA is working to implement the mandates issued by Secretary Johnson at the time of the report's release. Ms. Olivier, I want to also thank you for being with us today, and look forward to hearing the perspective of the American Association for Airport Executives on this report and these important issues. Your ideas and knowledge of the collective sentiments of airport executives across the Nation will add tremendous value to this discussion.

Lastly, I would like to thank Mr. Grossman, the CEO and executive director of Jacksonville International Airport and member of Airports Council International-North America, who will explain how one individual airport handles access control and insider threats issues. I understand that your airport participated in the 2008 100% employee screening pilot program, and I'm eager to hear about that experience.

I also understand that your airport employs unique strategies to mitigate the insider threat, such as yearly background checks from surrounding States, and I'm eager to hear about that as well. Certainly, every airport in this country is different and there is no one cure-all solution—but I think we may be able to draw best practices from your experience that could enhance the security across our aviation system.

Mr. KATKO. Thank you, Miss Rice.

I will now recognize myself for 5 minutes to ask questions.

Mr. Carraway, there are many areas that I think that we all agree on, so I want to kind of delve down into how we make what we agree on reality. The area I see the most difficulty trying to set parameters on is the security screening and inspection aspect. When I say set parameters, I think it is important to have some sort of general parameters within which all must operate to ensure that there is some sort of uniformity Nation-wide.

Now, on the same token, I am mindful of the fact that every airport is different. They are physically different. Kennedy Airport cannot be handled the same way as Syracuse, New York, where I am from, or an airport in a smaller city, or like Atlanta even. They are all different. I know Atlanta is endeavoring to many of the things talked about in this report, including 100 percent screening. But it is still the question: What is screening?

You talked about random screening as an option, but the committee has a strong desire, I would say, overall, to set some sort of general parameters for each of the employee entrance points to begin with. You can overlay that with random screening on the job in different areas inside the secure area and outside the secure area. But that critical point when they go from the non-secure to the secure area is what we are probably most concerned with.

So I want you to kind-of address that for us and tell us what you think employee access points should look like. Be mindful of the fact that we want to have some sort of general parameters for each of the employee access points, give airports the option of how many they want to have, but at least have some general standards within which they have to abide. So with that proviso, could you help us out here a second?

Mr. CARRAWAY. Yes, sir. Thank you very much again for this opportunity.

Chairman, the issue that you are addressing was taken very, very seriously by the ASAC. In fact, I would say that that was probably the most critical issue. In referring to the ASAC report, they indicated specifically that this report was based upon looking at the employee coming to work, doing their work, and also then leaving from work. So it was very important for them to consider exactly what would happen to that employee in the aspect of their operation.

In addition to that, they realized that every airport was different, that one size didn't fit all, utilizing the risk-based security perspective in doing so. Also, that they wanted to make certain that the employees felt that any time, at any place that they would have this feeling that they would receive screening and/or some inspection in some form or fashion.

That is the basis of the randomness that they brought to the table in the ASAC report and one that we have continued to do even today and which, immediately following the incident, we felt there had to be some sort of, again, this randomness that occurred so that every airport employee would have this feeling that they would be inspected in some form or fashion.

That is truly the basis of what the risk-based security initiative is truly about, because, as you well know, the screening that is done on the front side of the airport is nowhere near that that can be done on the back side. The infrastructure, as you say, is not the same, cannot be fitted in that form or fashion. But creating an environment where they can be feeling that they could be screened at any time is what we are going for. So that is what we are doing and exactly what the ASAC members have stressed for us to do.

What that looks like by the way of resources, it means our individuals, our TSOs, or BDOs, our behavior detection officers, it can also means canines, canines as well. Some airports have even gone on their own to do this themselves, in addition to the support that we bring to the table. My discussions with many airport directors and airports is that they felt this was significant for them to do and have begun to do it on their own.

Mr. KATKO. Yeah, I understand that, but maybe I am hung up on the physical composition of what the entrances should look like. Because I agree with everything you have just said, and I agree with what the ASAC is saying, but if you are screening someone after they are already in the secure area it may be too late. If you are screening before they get into the secure area that is great, but there is still that point where they enter in that there should be some sort of threat, if you will, or randomness to the access that they are going to get searched possibly coming into the secure area, and that is what I want you to address.

Mr. CARRAWAY. Well, unfortunately, there isn't this 100 percent place for every employee to go through. I think that is really evident by the ASAC's report.

What happens for most employees when they get there is there is either a biometric that is used, a swiping that is done, or a biometric using their hands, like in Dallas, that is done that allows them into that access area. There are some places in the airport, specifically Orlando and Miami, that they are doing some employee screening. But you have to realize, again, it is not 100 percent employee screening, there are some exceptions even to that rule, because there is equipment that has to be brought in, there are tools that are accessed there.

Chairman Katko, what I think I really would like to do is change the narrative, because I think we get so hung up on this 100 percent screening initiative that we miss the dynamic that truly is here. That is, as you said, the insider threat issue. So to change that dynamic requires this cultural change across the whole system, exactly what Miami and Orlando have done, created a culture where every employee believes that any time they could be screened. By having this randomness inserted into that process, that can happen.

Mr. KATKO. Thank you. I have so many more questions, but I am not going to hog the time. My time is up, and I now yield to Miss Rice.

Miss RICE. So, Mr. Carraway, let me ask you this: Do you think that there are any additional recommendations that you would make to increase security in this regard other than the ones that were suggested in the report?

Mr. CARRAWAY. At this time, I believe that the ASAC committee has done a very thorough job in identifying the issues for us, to include the criminal history checks. Recurrent history checks I think are very central to this as well.

Miss RICE. So that to me is one of the most glaring vulnerabilities that existed prior to this. Why was that?

Mr. CARRAWAY. Well, this was a trusted population, a trusted group of individuals. As you well know, airport airline workers are a unique bunch. They really are quite extraordinary about their work and prideful in what they do. Unfortunately, there are a few that took advantage of that, and that is what has brought us here today. I still believe they are a very professional group of very, very high integrity, and that is why it is important to institute the "See something, say something" and try to change that culture within the aviation worker industry.

Miss RICE. So who do you think does it best?

Mr. CARRAWAY. Who does it best? I mean, is there one that you would say gets as close to best practices? I don't know if there is an answer to this. There may not be. I am just curious as to whether there is one that you think represents really what best practices should be.

Mr. CARRAWAY. I think there are security levels at each area. I have been to practically all 450 airports. I can tell you that each one of them has a level of security that I would tout as very best practices. You have to understand that the ASAC committee is made up of just those individuals, and what they brought to the table were all of those best practices that they are familiar with and aware of in the industry.

I know we have touted Miami and Orlando to have initiatives out there. They are just a compendium of best practices. I think what we are going to do is take a look at all of those things over time and bring the very best to the industry, because at the end of the day we want the industry to be safe and secure.

Miss RICE. Well, there is no question about that. I think everyone would agree that everyone in this room, we are on the same team. We are not opponents in this.

Mr. CARRAWAY. Yeah, yeah.

Miss RICE. Will you tell me, would you agree, that there really isn't a one-size-fits-all, that the airports are different, uniquely different in their own ways? Would you agree with that?

Mr. CARRAWAY. I couldn't agree with you more. One size does not fit all. That is the crux of what they have brought to the table as well, to make certain that we find the best of all of those best practices. Something that may work at a large Cat X like Chicago may not work at a small Cat 1 or even smaller in North Dakota or in Iowa, not that those are——

Miss RICE. Thank you, Mr. Carraway.

Mr. CARRAWAY. Yes, ma'am.

Miss RICE. Thank you, Mr. Chairman.

Mr. KATKO. Unfortunately, they have called votes, but I think we can probably squeeze in one more 5-minute line of questioning. If Mr. Ratcliffe is ready, we will do that, and then we will break.

Mr. RATCLIFFE. How about if I talk fast?

Mr. KATKO. You will be just like me.

Mr. RATCLIFFE. Thank you, Chairman Katko, Ranking Member Rice, for holding another important hearing on this issue.

Thank you, Acting Administrator Carraway, for your testimony and for coming back to the committee. Clearly, since 9/11, Congress has entrusted TSA with the safety of Americans as they travel this country. As the gentlelady from New York commented, there have been a number of incidents fairly recently that have called into question the ability of airport employees to circumvent screening mechanisms. She talked about the incident, I think, at Atlanta Airport involving a Delta Airlines' employee smuggling firearms, but just in January there were two additional incidents, one with an FAA administrator, safety inspector, with a gun in his carry-on bag, and then also a Delta gate agent boarding a flight to Paris after circumventing passenger screening.

So all of this begs the question: How can we truly have a secure airport when employees are not fully vetted to the same standards that passengers are? So, Mr. Carraway, I want to talk a little bit about the process here and give you an opportunity to explain how static security measures in your opinion are better-suited to screen airport employees than 100 percent screening.

Mr. CARRAWAY. Sure.

Mr. RATCLIFFE. If you believe that.

Mr. CARRAWAY. Yes, I really do. I know this comes down to a random versus static or 100 percent employee screening, but we will never have the resources, sir, to ever fill up every doorway and access in the airport. That is why one of the recommendations of the ASAC committee was to look at those access points in the airport and with a recommendation to close those or to find ways to limit the number of access points in the airport.

Again, that strengthens the position of airport employees, having the realization that wherever they may be, they could be required to go through inspection or screening of some sort. That is the real strength of it: At any time, at any place that could occur.

So that is the real strength of it. Having the resources and the dollars put towards 100 percent employee screening seems to be out of balance, both from my perspective, as well as from the ASAC review.

Mr. RATCLIFFE. Okay. So let me ask you a little bit about the security process as it exists right now. Right now, an airport employee undergoes a background check where their fingerprint is cross-referenced with a criminal history background check. Is that right?

Mr. CARRAWAY. Yes, sir.

Mr. RATCLIFFE. Okay. Are there any other checks in place right now?

Mr. CARRAWAY. Yes, they also go through a terrorist screening base as well, and other security processes that we have through TSA. Also in the criminal history background there are certain qualifiers or offenses that will eliminate them from the process of being hired as well. So that information then goes back to the airport.

Mr. RATCLIFFE. Okay. But is it fair to say that this only happens one time?

Mr. CARRAWAY. Yes, that is the inefficiency of the system, yes.

Mr. RATCLIFFE. Okay. At some point in time didn't TSA inform the House Homeland Security Committee, this committee, that it was interested in implementing the FBI's Rap Back service?

Mr. CARRAWAY. Yes, sir.

Mr. RATCLIFFE. That being the case, as I understand that, that is where the employer would receive immediate notification if there was evidence of some criminal activity. That being the case, can you tell us the status of where TSA is with respect to that?

Mr. CARRAWAY. We are looking at that program and any others that would come to our attention that would allow us to do this recurrent, on-going vetting of employee criminal history status. The idea, obviously, is if they are involved in any arrests or warrants or prosecution that would happen, the airport would be immediately notified of that offense and could take action towards that individual or individuals for the crime.

Currently, Rap Back is being reviewed. It is not fully vetted and possibly on par to be implemented at this particular time. It takes a technology whole review, and implementation of that system would require both TSA and others to change their system to do that. That is why we have implemented the 2-year implementation or review of the criminal history at the airport, and we issued a security directive yesterday for all airports to do that immediately.

Mr. RATCLIFFE. Okay. Thank you, Mr. Chairman. I see my time has expired. I yield back.

Mr. KATKO. Thank you very much, Mr. Ratcliffe.

Unfortunately, as I noted, votes were called. We stretched out as far as we can. There are three votes. The first vote is going, a few minutes left, then there are two 5-minute votes. So we are going to take a recess subject to the call of the chair, but I can tell that as soon as we are done voting, we are coming right back and going to get right back at it, so a minimal delay for you all.

Mr. CARRAWAY. No problem, sir. Thank you.

[Recess.]

Mr. KATKO. The committee will come to order. I want to thank you for indulging us in getting our votes. We endeavored to get back as quickly as possible, and I am not getting used to this humidity here. It is brutal, and it is just starting.

Mr. Keating is up next.

Mr. Keating, please. You have 5 minutes.

Mr. KEATING. Thank you Mr. Chairman.

Thank you for waiting, Administrator Carraway.

Administrator, November 2010, before I was in Congress, I was a district attorney, a 16-year-old, Delvonte Tisdale, snuck into the tarmac at Charlotte Douglas Airport, and he hid himself in the wheel well. I know this because, unfortunately, he met a tragic end. The altitude froze him. They put the landing gear, he perished falling 30,000 feet in my district.

When I came here, I started asking questions about airport security as a result, because if a 16-year-old with no evil intent can do that. He didn't even show up in the video afterwards, when our police went to investigate the issue.

Now, since then, there has been somewhere in the vicinity of over 1,000 breaches. In that period that I look back with the latest statistics, 2004 to 2008, incredibly, I found out in terms of the security reviews that were done, the vulnerability assessments, that 87 percent of the airports weren't subject to that kind of security review.

So I brought it up with then-Secretary Napolitano. We have had other instances. We had a 15-year-old boy in California who stowed himself away in a wheel well. Fortunately, he lived and survived going to Hawaii. We had a Chicago man throw his bike over the perimeter fence and ride across the runway terminal to the door.

In Philadelphia, a man drove through a SUV, in the security fence there, and he drove across the runway as a plane was trying to land. In Los Angeles, a man climbed the perimeter fence 8 times within a year and twice reached the stairway in the tarmac. In Florida, a man running from law enforcement climbed the perimeter fence and hid in an empty plane. I mean, I could go on and on and on.

So I followed what has been done by TSA to try and deal with this issue, and I found out that for fiscal year 2011 to 2013, 30 airports were assessed annually. It is going down instead of improving. In 2014—I just got these figures a short time ago—that the assessments for that whole year were only 12 airports in the entire country, of approximately 450, as you mentioned. That is less than 3 percent.

So over 97 percent of our airports aren't even getting this kind of security review. It is getting worse instead of better. Yet we are putting so much attention at the gate that, in fact, it is getting worse in the perimeter. Now, how tough is it for someone, if a 15- and 16-year-old can do these things, for someone to put a bomb there, a terrorist with a different kind of intent?

How can this continue to happen and, in fact, go in the opposite direction? We had a field hearing on this with the committee, with Chairman McCaul and myself when we were head of Oversight. We knew the jurisdictional issues. We talked about the perimeter issues. We have had expert after expert after expert, including 9/11 Commission members, and they said it remains one of the top security threats that we have.

Yet, it is getting worse. We are not even doing 3 percent. My patience is gone on this issue. Something is going to happen, and we are not doing anything about it. If you hear frustration, it is real.

Mr. CARRAWAY. I understand.

Mr. KEATING. So I know you are the acting administrator, I am not putting it on your doorstep, because this is happening for years. But something has to be done before we are reacting to a terrorist attack and a tragedy.

Mr. CARRAWAY. I thank you for the opportunity to address that, and it is a concern for TSA as well as the airports as well.

The enormous responsibility of protecting perimeters is a combined effort both between TSA and the airports. No one owns it totally. Yes, we do the JVAs and we have increased the number of JVAs over the years. Yes, we are still ramping up that, particularly on a risk-based security perspective.

Mr. KEATING. I hate to bother you, but this is GAO information. It is going down.

Mr. CARRAWAY. Well, we are looking at it on a risk-based security perspective, hitting those airports that we deem to be the most at-risk airport. It is a matter of resources, as you can well imagine. Doing a joint vulnerability assessment with the FBI is an enormous task in doing. You don't look at just the perimeter, you look at every operation that is within the airport's purview to do that.

Perimeter security is an enormous issue. There have been millions and multimillions of dollars spent on security systems, and still they are penetrable by individuals. The fact that someone could use a boat and come across and into Kennedy Airport is just an indication of that, and they have spent multi-million dollars on intrusions systems.

I think the takeaway truly is that there are still layers in support of the airport and perimeter environment. Although someone made it through the fence and reached an airport or an airplane, there is still law enforcement, there is still some other capacity issues that are in place to assure that nothing further gets done. By just simply getting inside the belly of an airplane, there is still going to have to be something done to create this catastrophic event that we are talking about.

Mr. KEATING. Well, if they couldn't pick up a 15-year-old boy or a 16-year-old boy, how are they going to pick up an explosive? I mean, you are saying that we are doing better. It is risk assessment. It is a network. You are doing less than 3 percent of the airports. Once a plane is in that network it can go to Charlotte and it is in the system. So it is vulnerable everywhere in that respect.

So I just have to tell you, something has got to be done. And fact that you said more is being done on perimeter security just doesn't match up to the facts. If you have facts that can prove me wrong, I want to hear them, but the numbers don't lie.

Mr. CARRAWAY. Well, I would simply tell you, we work very hard with the airports to deal with perimeter security. We discuss it constantly. We know that there is not one-size-fits-all, and exacting one solution is not going to keep someone with intent of doing something in that airport environment. That is why we have layers of security, both from TSA and the airport's perspective.

Mr. KEATING. Well, the layers are not working in this instance. I have got to tell you, discussing it is great, but it is time to do something about it.

I yield back.

Mr. CARRAWAY. Thank you very much, sir.

Mr. KATKO. Thank you very much, Mr. Keating.

Seeing no other Congressmen and -women, I want to follow up on some of the questions before we let you go, Mr. Carraway.

One thing I want to do at the beginning is make a point of clarification. I think you mentioned in your comments in answering some of the questions that we were looking for 100 percent screening. That is not the case.

What I was envisioning and what we as the committee are envisioning with respect to these employee entrance points is that if employees go through a certain point, a select number of them may be randomly selected at any time, whatever the ratio may be, and that we can work out—in fact, we should probably talk for a moment at some point before you are done here today—but the idea is that when they come into the airport screening, they are going from the nonsecure to the secure area, that critically transitional point, that there is some sort of threat at that point that they are going to get searched, not just swiping a card.

I understand that there are costs involved, and in the next session we will be talking with the airport people and they are going to tell me, "Are you nuts?" because it is going to cost too much money. I understand that. We will get to that, and we want to work with them on that. But I am curious to see what you think of that concept.

Mr. CARRAWAY. I see what you are saying.

Mr. KATKO. Okay.

Mr. CARRAWAY. Yeah, let me clarify, and maybe I didn't express it very clearly. The randomization is a full gamut of activities that the airport and TSA will employ as an individual comes to work. In some locations, it could very well be a magnetometer. It could be very well at an airport location electronic trace detection equipment of testing someone's hands. It could be an array of someone just simply looking into their bags or asking, verifying with their identification card to certify who they are.

The ASAC, as well as TSA, did not want to limit that range of suites of activities for an employee coming to work that day. That too increases the randomness and the opportunity and expectation that an individual will be inspected when they come to work and even possibly as they exit the airport environment as well.

I a bit misunderstood where you are coming from, from that, but that is how it is going to look across the network.

Mr. KATKO. Okay. So what do you think the employee access points should look like? What are the minimum requirements you think we should have at those access points?

Mr. CARRAWAY. That is a discussion I think would be best to have with the ASAC. At this particular point, it has not come to a point of requiring a minimum standard.

I can tell you from a law enforcement perspective, I didn't want to tie anyone's hands, to say this is what you are going to have to get, because I think it is an unfunded mandate, and we didn't want to do that.

We have had such great success in having communication and discussing with our stakeholders and our partners about this issue. If they find the need, most of them have literally gone out and taken care of those responsibilities without TSA having the authority to say: This is an SD, here is the directive, go forth and do those things.

Mr. KATKO. Okay. All right. Well, we will follow up on that with the next panel.

We have talked a lot about screening inspection and risk-based security aspects. We could probably go on for a while with that, but I want to touch on a few other things before we are done here. Talk for a moment about the vetting of employee and security threat assessments.

There has been some talk in the ASAC report, and I just want to know if the recommendations with respect to the vetting of employees are something that you agree with and increasing the vetting and the randomization and recurrent vetting, et cetera.

Mr. CARRAWAY. This is a very important step. I think, as you can tell from the ASAC report, that they very much agree with it, and we have too. Having that recurrent vetting gives us a level of security about who and what the individual has been involved in. Couple that with looking at their past history, criminal activity, if any concerns, is another critical component of that.

Mr. Chairman, working with you and others to help solidify that with those disqualifying criteria would be very helpful. In addition, strengthening the time frame of those disqualifying offenses would be very helpful as well.

But the first component is doing that recurrent vetting process, whether or not it is the FBI's Rap Back initiative or some other recurrent vetting process that we take advantage of. That is just the very first step to assure the safety and knowledge of who that airport worker really is.

Mr. KATKO. Yeah, understood. Because with respect to the Delta Airline employee, if they went back a little further, they would have found that he had some convictions that were relevant to his criminal conduct. I think that is part of it, going back farther, doing the social media aspect of it as well. I think that is something we all agree on and so that is not really a controversial point. So I think that we will move on.

Briefly, with respect to the internal controls and auditing of the airport-issued credentials, you agree with the recommendations as well in the ASAC report?

Mr. CARRAWAY. Yes, I do. Again, that is another critical component. Many times we find individuals who have had the opportunity, they may have been discharged for some activity at one end of the airport and by the end of the day they are hired at another end of the airport. Having that critical information about that individual is very essential to the airport as well as TSA, and we will have a database established to have that information and share with the airport environment.

Mr. KATKO. Now, the next category I just want to touch on is risk-based security for higher-risk populations and intelligence.

Mr. CARRAWAY. Yes, sir.

Mr. KATKO. Now, of course, this was touched on in the report as well. What do you think about that?

Mr. CARRAWAY. Again, it is another critical aspect for securing the airport. We believe sharing of information with our partners is essential to securing the airport. We already have intel briefings and FIOs, our field information offices that share information with the airports and the like. But I think we can do an even better job in sharing that information, and we are looking at ways in which to do that.

Mr. KATKO. Okay. Then last, the security awareness and vigilance, the proverbial "if you see something, say something" campaign, I think that, to me, is no-brainer that everyone agrees with, to encourage them to speak up. The question is: Do you think we should establish a hotline to DHS, or how do you want to do that?

Mr. CARRAWAY. Yes, we are looking at establishing a hotline specifically to TSA at this particular point and to create even an anonymous reward effort through the airports if necessary. All of these things in conjunction, "see something and say something," will help to secure and create that culture that I spoke about earlier.

Mr. KATKO. Okay. Now, I know you are all happy that we are not coming out here saying you have to have 100 percent employee screening, and I am sure that is a good thing, but at the same time we are still, I don't know if hung up is the right term, but we are concerned about the fact that there has got to be some sort of uniformity that is applied Nation-wide that is flexible enough to deal with the different airports, because I know that airports are different all over the country.

So that is a discussion we are going to have to have going forward. I don't know if we need to have another hearing. Perhaps we may just call you back in a panel discussion type of thing after I raise these issues. So between now and that time I reach out to you again, I want you to kind of think more about it with your people in Homeland Security about what it is we can try and memorialize that would at least set some sort of parameters for the employee access point.

That seems to me to be the biggest sticking point. I mean, there are people that say it should be 100 percent employee screenings, everyone goes through magnetometers. I understand the costs involved with that.

But I also realize and acknowledge that I probably don't sound much like a Republican when I am saying this, but we can't worry just about the cost of things. When it comes to security, if there are things that should be done, we have got to find a way to find the money through offsets to keep our country and our airlines as safe as possible.

So we probably will revisit this issue with you either formally or informally, so I guess I am going to ask you to chew on it going forward and we can talk more about it.

Mr. CARRAWAY. Mr. Chairman, can I just simply say, thank you for your comment and obviously your diligence in seeking this issue, because I can tell you, those behind me and the other airport and airline executives and workers feel the very same way about this issue. This is the environment that they work in. They are very proud of what they do. They want to make certain that their environment is safe and secure as well.

So thank you, and I look forward to working with you and others in this regard.

Mr. KATKO. Well, I appreciate that. I will close by noting, again, what I said at the outset, and that is, it was heartening to know that at the beginning we identified an issue and everyone said, yes, it is something that needs to be worked on, and we are all working towards the same goal here. That is a good thing. No one had to yell at each other, so that is a good thing.

Mr. CARRAWAY. Thank you, sir.

Mr. KATKO. So thank you very much, sir, and have a good evening.

Mr. CARRAWAY. Thank you.

Mr. KATKO. The committee will stand in recess for just a few moments.

[Recess.]

Mr. KATKO. The Chairman now recognizes the second panel.

Good afternoon. We are pleased to have another panel of distinguished witnesses before us today. Let me remind the witnesses that their entire written statements will appear in the record.

Our first witness, Ms. Jeanne Olivier, is an assistant director of the Security Operations and Programs Department of the Port Authority of New York and New Jersey and is testifying on behalf of the American Association of Airport Executives. I will note also that she is an avid statistician, which horrifies me, because I really struggled with that in school.

So welcome to our arena.

The American Association of Airport Executives is the world's largest professional organization for airport executives, representing thousands of airport management personnel at public use, commercial, and general aviation airports. Ms. Olivier has worked with the port authority for over 30 years in airport operational management positions at JFK International, LaGuardia, Newark Liberty International, and Teterboro Airports.

The Chairman now recognizes Ms. Olivier to testify.

STATEMENT OF JEANNE M. OLIVIER, A.A.E., ASSISTANT DIRECTOR, AVIATION SECURITY AND TECHNOLOGY, SECURITY OPERATIONS AND PROGRAMS DEPARTMENT, THE PORT AUTHORITY OF NEW YORK & NEW JERSEY, TESTIFYING ON BEHALF OF THE AMERICAN ASSOCIATION OF AIRPORT EXECUTIVES

Ms. OLIVIER. Thank you, sir.

Chairman Katko, Ranking Member Rice, Members of the subcommittee, thank you for the opportunity to be with you today. I am testifying, as you said, on behalf of the American Association of Airport Executives, which represents thousands of men and women across the country who manage and operate the Nation's airports. I am actively involved with AAAE as the chair of the association's Transportation Security Services Committee.

Mr. Chairman, airport executives want to assure you and all of the Members that we take recent incidents and the prospect of the insider threat very seriously. Airports are public entities with their own security responsibilities, and they meet those obligations with a focus on the need to protect public safety, which is a fundamental mission of all airports.

Collectively, airports have invested billions of dollars since 9/11 to enhance security with meaningful results. Perhaps as important as the financial investment is the resolve that airport executives have to enhance security every day. My fellow colleagues and I are public servants, sir, and we take our charge to protect public safety and security, be assured, very seriously.

The security imperatives of airports and the TSA are closely aligned, and collaboration between the two to enhance the layers of security that exist and to identify and address potential threats in the airport environment is quite essential. Our work together continues to evolve and improve, as Acting Administrator Carraway has described just a few minutes ago, and we are confident that even more progress will be made in the days ahead.

In our view, we have an important roadmap on how to proceed thanks to the work of the Aviation Security Advisory Committee's ad hoc working group that was established in January to review employee screening and airport access control. I was fortunate to serve as a subject-matter expert on the working group, joining several of my airport colleagues in that effort, along with a number of professionals from law enforcement and the aviation and security industries.

The group in early April provided TSA with a report outlining 28 recommendations that collectively take a risk-based and multi-layered approach to employee screening and airport access control with shared responsibilities across the aviation community. Specifically, the ASAC recommendations cover employee vetting, random security screening and inspection, internal controls and audit of badges, risk-based security for higher-risk employee populations, intelligence and intelligence sharing, and security awareness and vigilance.

As you know, Secretary Johnson recently outlined several immediate actions based on the recommendations of the working group that the aviation industry is now working to comply with. We were all gratified to hear Acting Administrator Carraway refer to the representations of the group as comprehensive, thoughtful, and promising in helping TSA achieve meaningful reforms in partnership with the aviation industry.

We couldn't agree more. The working group approached this task with a seriousness of purpose and determination that reflects what we believe Congress had in mind when it codified the ASAC last year. We believe firmly that the final ASAC recommendations offer a roadmap of how TSA and industry can partner together to enhance security and mitigate the insider threat and other potential vulnerabilities highlighted by the events that led to the establishment of the working group in the first place.

Before closing and moving to answer any questions you may have, I would like to make just a few final points.

No. 1: The ASAC process. We believe it worked incredibly well, bringing a wide array of industry professionals together to partner with TSA in producing recommendations for how to effectively deal with security threats with meaningful, actionable, and implementable solutions.

No. 2: What is next? We urge Congress and DHS to recognize and support the important work of the ASAC and avoid the temptation to pursue other approaches in legislation or otherwise that could divert resources from other critical security functions.

No. 3: Cost in operations. As efforts continue to address the insider threat and other potential vulnerabilities, Congress and DHS must work to minimize the financial and operational implications that new requirements, individually and collectively, will have on airports and the aviation industry. In a world of limited resources, we must proceed smartly with Federal backing when possible.

In closing, please allow me to offer my sincere thanks to the TSA for its work in providing the resources necessary to ensure that the ASAC process was successful and to the subcommittee for your continued engagement on these important issues. I appreciate being here, sir, with you today, the committee, and look forward to answering any questions you might have.

[The prepared statement of Ms. Olivier follows:]

PREPARED STATEMENT OF JEANNE M. OLIVIER

APRIL 30, 2015

Chairman Katko, Ranking Member Rice, and Members of the subcommittee, thank you for the opportunity to be with you to discuss airport access control—an important security function that local airport operators have held for decades in accordance with strict Federal standards, requirements, and oversight. I am testifying today on behalf of the American Association of Airport Executives, which represents thousands of men and women across the country who manage and operate the Nation's airports. I am actively involved with AAAE as chair of the Association's Transportation Security Services Committee. In addition to my work with AAAE, I currently serve as assistant director, aviation security and technology for the security operations and programs department of the Port Authority of New York and New Jersey. In this capacity, I oversee security operations for New York's Kennedy and LaGuardia airports and for Newark Liberty International Airport and Stewart International Airport.

Mr. Chairman, I want to assure you and Members of the subcommittee that airports take recent incidents and the prospect of the "insider threat" in the aviation environment very seriously. Airport executives are working constantly in collaboration with the Transportation Security Administration to enhance the layers of security that exist to identify and address potential threats in the airport environment.

In addition to partnering with TSA to help the agency meet its primary mission of passenger and baggage screening, airports as public entities also perform a number of inherently local security-related functions at their facilities, including incident response and management, perimeter security, employee badging and credentialing, access control, infrastructure and operations planning, and a myriad of local law enforcement functions. These important duties have long been local responsibilities that have been performed by local authorities in accordance with Federal standards under Federal oversight.

Airport operators meet their security-related obligations with a sharp focus on the need to protect public safety, which remains one of their fundamental missions. The professionals who perform these duties at airports are highly trained and have the first responder duties that I know each and every Member of this subcommittee, the Congress, and the country value immensely. From a security and resource perspective, it is critical that these inherently local functions remain local with Federal oversight and backed by Federal resources when appropriate.

AVIATION SECURITY ADVISORY COMMITTEE WORKING GROUP REPORT ON AIRPORT ACCESS CONTROL

I also recently served as a subject-matter expert on the Aviation Security Advisory Committee's ad-hoc working group to review employee screening and airport access control. I was honored to join my other airport colleagues who also served on the group, including Jan Lennon from Atlanta Hartsfield-Jackson International Airport, Michele Freadman from Boston Logan International Airport, Cedric Johnson from BWI Thurgood Marshal International Airport, Alan Black from Dallas Fort Worth International Airport, and Chief Stephen Holl from the Metropolitan Washington Airports Authority Police Department, as well as staff from AAAE and ACI–NA. In addition to airport operators and airport associations, the working group was comprised of a broad cross-section of industry representatives, including air carriers, airline associations, labor, law enforcement, general aviation, security technology, and airport services providers.

In a letter dated January 8, TSA Acting Administrator Mel Carraway asked the ASAC to evaluate the aviation industry's current approach to airport employee screening and to review other risk-based approaches to address potential vulnerabilities related to security in the sterile area, including policy and procedures, industry best practices, technology, and employee training. TSA tasked the working group with providing 30-day, 60-day, and 90-day reports. The working group's final 90-day report was submitted to TSA on April 8 after approval by the full ASAC.

The working group's report outlines 28 recommendations that collectively take a risk-based and multi-layered approach to employee screening and airport access control with shared responsibilities across the aviation community, including TSA, air carriers, and airport operators. Specifically, the ASAC recommendations cover employee vetting; random security screening and inspection; internal controls and audit of badges; risk-based security for higher-risk employee populations; intelligence and intelligence sharing; and security awareness and vigilance. I have attached the list of recommendations to the end of my statement.

Due to the interdependent nature of each of the recommendations and the complex variables associated with each one, the working group did not have the time to prioritize the recommendations. Time constraints also limited our ability to provide detailed cost analysis. The working group urged TSA to base any future actions related to employee screening and access control on these community-driven recommendations. The group also made clear its belief that any action taken by TSA should be made through the established regulatory process.

The report contains a discussion and analysis of 100 percent employee screening, concluding that 100 percent physical screening would not completely eliminate potential risks and could divert limited resources from other critical security functions. Recent studies have indicated that implementing a 100 percent physical screening approach would cost an estimated $15 billion annually and could cause significant operational disruptions at many airports. As a result, the working group developed their recommendations within the context of Risk-Based Security (RBS), a comprehensive approach to aviation security endorsed by the Department of Homeland Security and TSA.

In this regard, the working group agreed that greater implementation of RBS is essential in continuing to shift the aviation security paradigm in a very positive and meaningful way. RBS replaces the old one-size-fits-all security system that was in place prior to the attacks of 9/11, and it has proven to be a significantly better system because it enables allocation of available resources where they have the greatest ability to reduce risk. It also is driven by identifying those with intentions to do harm.

The working group applied risk management principles in considering aviation's exposure to the insider threat and developed appropriate mitigation strategies within the current and proposed budgetary framework. The working group exercised a RBS approach that employed a systematic process of understanding, evaluating, and addressing these risks to mitigate the exposed vulnerabilities and to close any security gaps in airport access control. The risk-based system for employee screening or access control encompasses intelligence, employee vetting, RBS based on higher-risk populations, security awareness, training and behavior analysis, as reflected in the final recommendations.

On April 20, as a result of the recommendations contained in the ASAC report, DHS Secretary Jeh Johnson directed TSA to take several immediate actions:

- Until TSA establishes a system for "real-time recurrent" criminal history background checks for all aviation workers, require fingerprint-based CHRCs every 2 years for all airport employee SIDA badge holders.
- Require airport and airline employees traveling as passengers to be screened by TSA prior to travel.
- Require airports to reduce the number of access points to secured areas to an operational minimum.
- Increase aviation employee screening, to include additional randomization screening throughout the workday.
- Re-emphasize and leverage the Department of Homeland Security "If You See Something, Say Something™" initiative to improve situational awareness and encourage detection and reporting of threat activity.

Airports and the aviation industry are working collaboratively with TSA to implement these requirements. And, while there may be a difference of opinion on the specifics of the short-term actions from DHS and the recommendations of the ASAC working group to TSA, I think it is important to highlight the success of the overall ASAC effort over the past few months and the opportunity it provides as a model for pursuing security enhancements in the future. Airports are very pleased with the collaboration and feel confident that we will achieve better results quicker by having Government and industry work together toward the shared imperative of enhanced security.

As the subcommittee contemplates further engagement and potential action to address the insider threat, we urge you to pay careful attention to the detailed work and recommendations of the ASAC working group. Congress and TSA have rightfully recognized the value of the ASAC and the promise of its approach in achieving real, implementable security enhancements.

OTHER INDUSTRY EFFORTS—ACCESS CONTROL AND PERIMETER SECURITY

In addition to my work on the ASAC, I serve on the RTCA Special Committee on airport access control, which in 2014 released the updated standard for airport access control (RTCA DO230–D). The document was prepared under the auspices of RTCA, which serves as a Federal Advisory Committee, and provides a vehicle for Federal regulators and regulated parties to develop consensus-based guidance and standards documents.

Notably, the RTCA document provides guidance on acquiring and designing airport security access control systems, testing and evaluating system performance, and operational requirements. It also incorporates the latest technological advances in security access control system and identity management. The major areas covered include: Credentialing; Biometrics; Physical Access Control Systems (PACS), Perimeter Intrusion Detection Systems (PIDS); Video Surveillance Systems; Security Operations Centers (SOC); Integrations; Communications Infrastructure; and General Acquisition-Related Considerations.

The 2014 document was the fourth version since the first standard for airport access control was published by RTCA in 1996. The Special Committee has spent the last year working on yet another update—no other airport security standard is updated so regularly. Like ASAC, the RTCA process involves the airport and aviation community working with TSA to provide consensus recommendations and a comprehensive set of guidelines on all technical aspects of access control. The document provides both TSA and airport operators a convenient source of information on current practices and procedures and unbiased information on new technology.

The comprehensive guidance document also contains an entire section on perimeter intrusion detection, which reviews options from patrols to state-of-the-art technology solutions and what factors airport operators need to consider when implementing a perimeter security solution at their facility. I would be pleased to discuss this important work with the committee in more detail.

Mr. Chairman, airport executives are working constantly in collaboration with TSA to evaluate and enhance the layers of security that exist to identify and address potential threats in the airport environment, including extensive background checks for aviation workers, random physical screening of workers at airports, surveillance, law enforcement patrols, robust security training, and the institution of challenge procedures among airport workers, to mention a few.

In our view, the best approach to enhancing access control at the Nation's airports moving forward lies with continuing to focus on robust background checks, maintaining our multi-layered security approach, and preserving and protecting the critical local layer of security that airports provide with credentialing, access control, and other local functions. Inherently local security functions should remain local with Federal oversight and backed by Federal resources when appropriate.

Members of the committee, recent events have highlighted the fact that we can never rest when it comes to airport security. Airport operators take their responsibilities in this area very seriously and are constantly seeking better approaches in close collaboration with our partners at TSA. I am confident that we can find productive ways to move forward, and I can assure you that the airport community is eager to partner with the subcommittee and all of you to achieve our shared goal of ensuring the highest level of security for the traveling public.

FINAL REPORT OF THE AVIATION SECURITY ADVISORY COMMITTEE'S WORKING GROUP ON AIRPORT ACCESS CONTROL RECOMMENDATIONS

Security Screening and Inspection

1. DHS should immediately shift existing resources, as needed, to expand the TSA's random employee screening/inspection program (i.e. the Playbook to secured area access points).

2. TSA, in coordination and collaboration with Government and industry subject-matter experts and airport and aircraft operators, should develop an employee access security model using intelligence, scientific algorithms, and risk-based factors. This model should give all employees the expectation that they are subject to security screening/inspection at any time while working at an airport.

3. TSA should establish risk-informed, enhanced random screening/inspection for all employees, which would be increased on the basis of identified risk.

4. DHS should request from Congress needed funding for implementation of security measures for a to-be-developed employee access security model and the Playbook.

5. Airport and aircraft operators should prominently post signage at access portals or via other means to alert employees that they will be subject to screening/inspection in order to support compliance with random screening/inspection programs.

Vetting of Employees and Security Threat Assessment

6. TSA should accelerate the implementation of the FBI/Next Generation Identification (NGI) Rap Back Service with an immediate pilot with airport and aircraft operators with a goal of full implementation by the end of calendar year 2015. Real-time recurrency should be part of the CHRC vetting process, similar to the perpetual vetting conducted by TSA for the STA.

7. TSA should review the existing list of disqualifying criminal offenses to ensure that it is comprehensive enough to address the current threat environment and pursue any legislative or regulatory changes needed to update the list of disqualifying criminal offenses, other eligibility criteria, the addition of permanent disqualifying criminal offenses, extending the look-back period, and starting the period of adjudication on the individual's sentence release date or program completion date.

8. Airport and aircraft operators should introduce new certification language for badge applications that broadens the focus from existing regulatory requirements to a greater focus on overall suitability.

9. Airport and aircraft operators, in coordination with TSA, should review current training for Trusted Agents and Signatory Authorities and, as needed, provide enhanced training on identification documents, identity fraud, and behavioral analysis.

10. TSA should create and maintain a National database of employees who have had their airport- and/or aircraft operator-issued badges revoked for cause.

11. A comprehensive review should be conducted by the TSA to enable a web-based portal for industry utilization for employee vetting by TSA.

12. TSA's Security Threat Assessment should be enhanced to include SSN, running all U.S. citizens against SAVE, fingerprints against DHS' IDENT system, TSA PreCheck Disqualifying Protocols, and run foreign nationals and foreign-born against international databases.

Internal Controls and Auditing of Airport Issued Credentials

13. TSA, and airport and aircraft operators should assess the efficacy of the auditing program requirements for airport-issued identification media (e.g., security badges) designed to ensure the integrity, accountability, and control of security media.

14. In cooperation with airport and aircraft operators, TSA should consider the establishment of biometric standards which may be used in identity verification and badge validation. Included in this effort should be recommended standards and a cost/benefit analysis focused on implementing any such standards.

15. TSA should implement direct enforcement requirements upon authorized signatories associated with non-compliance, to include failure to immediately report lost, stolen, and unaccountable employee badges and employee separations.

16. Airport operators, in conjunction with tenant business partners, should identify opportunities to further restrict access privileges and/or further reduce access points as operationally necessary.

17. TSA, in coordination with airport and aircraft operators, should support the enhancement/expansion of CCTV or other measures to monitor employees at certain entry points and other areas, as necessary.

RBS for Higher-Risk Populations and Intelligence

18. To foster the effectiveness of employee screening/inspection, TSA should consider the development of risk matrices for various employee groups using RBS principles.

19. TSA should maximize the dissemination of Sensitive and Classified intelligence collection as widely as practicable.

20. TSA should further explore the use of social media to track and assess emerging threats that may pose a risk to aviation. Analysis and best practices gained from this effort should be disseminated to regulated parties.

21. TSA should expand/improve the existing City and Airport Threat Assessment (CATA) or similar program to capture, quantify, and apply applicable in-

telligence information, and engage the aviation community in developing mitigation measures.

22. TSA should partner with airport and aircraft operators in conducting the Airport Risk Evaluation (A.R.E.) and provide the results of any and all risk and vulnerability assessments to appropriate regulated parties within the aviation community.

23. TSA should further analyze applicable insider-threat cases to create a model of predictive risk factors based on research and applied knowledge of the involved individuals and techniques used to circumvent security measures.

24. TSA, FBI, and CBP should provide and make available enhanced training and information on insider threat activity and suspicious indicators that could be incorporated into airport and aircraft operator training programs.

Security Awareness and Vigilance

25. TSA should consistently provide briefings to airport and aircraft operators on the results of their security assessments to provide awareness of potential risks at the airport.

26. Airport and aircraft operators should be encouraged to develop and implement employee engagement/recognition programs aimed at promoting employee engagement in aviation security.

27. TSA, and airport and aircraft operators should promote existing National anti-terrorism reward/employee engagement programs to increase security awareness and reporting of suspicious activity.

28. TSA should promote or establish an existing or new Anonymous Tip Line to receive information from aviation employees who report a security concern or incident, and direct it to the appropriate regulated party(ies).

Mr. KATKO. Thank you, Ms. Olivier, for your testimony. We appreciate you being here today as well.

Our second witness, Mr. Steven Grossman, currently serves as the chief executive officer and executive director of the Jacksonville Aviation Authority and is testifying on behalf of Airports Council International, North America. I don't know if he is going to shed some light on who Jacksonville is going to select tonight in the NFL draft, since they have a high draft pick, but maybe we can talk off-line about that.

But the Airports Council International, North America, represents local, regional, and State-governing body that own and operate commercial airports in the United States and Canada. Mr. Grossman assumed his role as CEO and executive director in 2009 and oversees the operation, maintenance, development, and marketing of all authority assets, which include Jacksonville International Airport, Cecil Airport, Jacksonville Executive at Craig Airport, and Herlong Recreational Airport.

The Chairman now recognizes Mr. Grossman to testify.

Mr. Grossman.

STATEMENT OF STEVEN J. GROSSMAN, CHIEF EXECUTIVE OFFICER/EXECUTIVE DIRECTOR, JACKSONVILLE INTERNATIONAL AIRPORT, JACKSONVILLE AVIATION AUTHORITY, TESTIFYING ON BEHALF OF THE AIRPORTS COUNCIL INTERNATIONAL, NORTH AMERICA

Mr. GROSSMAN. Thank you, Chairman Katko, Ranking Member Rice, and Members of the subcommittee. Thank you for the opportunity to provide a perspective of both an airport operator and that of Airports Council International, North America, on airport access control measures.

For airports, the safety and security of passengers, employees, and facilities are top priorities. Airports are in full compliance with

Federal requirements and work closely with the Transportation Security Administration and airline partners to examine, test, and refine the aviation security system to provide the optimum level of security.

TSA Acting Administrator Carraway is a strong leader and his team is always willing to partner with airports on security initiatives. In addition, we appreciate the opportunity for ACI–NA and airports to participate on the Aviation Security Advisory Committee review of access control.

Criminal acts involving the unauthorized transportation of guns on aircraft prompted calls for the TSA to mandate 100 percent screening of employees. As we have talked about, 100 percent employee screening does not translate to 100 percent security and is simply the wrong approach. A low-employee screening is one of the multiple players of the aviation security system. It is not a standalone solution and should not be viewed as a silver bullet.

In 2008, the Jacksonville International Airport and six other airports participated in an employee screening pilot program. During the pilot, only one prohibited item was discovered. Checkpoint screening operations were impacted. Construction was also disrupted, as it was necessary to devote resources to promptly screen the drivers and cement vehicles in order to prevent the cement from hardening before it could be delivered.

As the ASAC appropriately noted, to implement 100 percent employee screening in the United States would be a significant investment of resources that would be unavailable to address other pressing threats. TSA has a random screening program called Playbook, which uses roving teams of TSA transportation security officers to conduct random and unpredictable physical screening of employees.

At the Jacksonville International Airport and other airports, access points have been reduced, airports routinely support Playbook operations to reinforce employees' expectations of being screened, and conduct random inspections of employees and their Security Identification Display Area badges. In addition, some airports, including Jacksonville, conduct additional background checks on employees when their badges are renewed or at other intervals.

TSA identified the need to implement risk-based, intelligence-driven initiatives that enhance security. Airports support the TSA PreCheck for enrolled travelers and other risk-based approaches that provide the flexibility to apply security measures in areas where they have greatest ability to effectively reduce risk. Airport perimeter security involves multiple layers of integrated processes, procedures, and technologies. The layers of security provide an effective system to deter and detect potential intruders.

In addition to perimeter fencing and controlled-access gates, frequent patrols of perimeters are conducted by airports and airline personnel, law enforcement officers, and other representatives. Employees are trained to identify and immediately report suspicious activities.

It is important to note that most of the perpetrators of recent breaches were promptly apprehended, and I think this demonstrates the effectiveness of the measures already in place, although more can be done. Reporting about lost and unaccounted-for SIDA badges provided no information about the security systems designed to mitigate potential vulnerabilities.

In addition to the badge swipe, many access control suspects require personal identification numbers to be entered to gain access through controlled portals. Furthermore, airports frequently reissue badges to all authorized employees upon receiving reports of lost or stolen identification media, badges—and badges are immediately deactivated.

Now I would like to offer five recommendations to further enhance the airport access control, and this is probably most important: Invest in intelligence. History has demonstrated that effective intelligence information and sharing plays a critical role and provides one of the best opportunities to identify potential threats and prevent terrorist attacks.

No. 2, continually review security requirements and eliminate those that are outdated. Based on such a review, adjustments can be made so that resources are applied in those areas where they can effectively reduce risk.

Immediately implement the FBI's Rap Back program so that we can have real-time information on security issues.

Further, expand the TSA Playbook program to provide for random screening.

No. 5, institute an airport security-focused grant program or modernize the PFC to provide readily available funding support for these types of security measures.

Mr. Chairman, thank you for the opportunity to testify, and I look forward to your questions.

[The prepared statement of Mr. Grossman follows:]

Prepared Statement of Steven J. Grossman

April 30, 2015

Chairman Katko, Ranking Member Rice, and Members of the subcommittee, thank you for the opportunity to provide the perspective an of airport operator as well as that of Airports Council International—North America (ACI–NA) on airport access control measures.

I am the CEO and executive director of the Jacksonville Aviation Authority and a member of the ACI–NA U.S. Policy Board, which is responsible for the formulation and direction of policy decisions arising under U.S. legislative and regulatory matters. As a member of the ACI–NA U.S. Policy Board, I have a profound interest in and advocate for risk-based aviation security initiatives that not only enhance security but also provide airport operators needed flexibility.

The Jacksonville Aviation Authority, an independent government agency created by the Florida legislature, operates the Jacksonville International Airport, Cecil Airport, Jacksonville Executive at Craig Airport, and Herlong Recreational Airport.

Located in Florida, Jacksonville International Airport has more than a dozen major airlines and a network of regional carriers that provide some 200 daily arrivals and departures. In 2013, the number of passengers using Jacksonville International Airport (JAX) reached 5,129,212.

Mr. Chairman, the safety and security of passengers, employees, and facilities are top priorities for U.S. airports. As such, the Jacksonville International Airport, and airports across the United States, are in full compliance with Federal requirements and, continually works with the Federal Government and airline partners to examine, test, and improve upon the aviation security system to provide the optimal level of safety and security. In partnership with the Transportation Security Administration (TSA), U.S. Customs and Border Protection (CBP), the Federal Bureau of Investigation (FBI), other Federal, State, and local law enforcement agencies, and airlines, airports maintain a comprehensive, multi-layered, risk-based aviation security system. In my testimony, I have included several suggestions to further enhance airport access control measures.

EMPLOYEE SCREENING

As a result of recent criminal acts involving the unauthorized transportation of guns on-board commercial aircraft, U.S. Department of Homeland Security (DHS) Secretary Jeh Johnson and TSA Acting Administrator Melvin Carraway requested that the Aviation Security Advisory Committee (ASAC) conduct an "expedient and comprehensive review" of access control measures to address potential security vulnerabilities at airports.

Tasking the ASAC to identify security enhancements was the right approach and ensured collaboration across the industry. ACI–NA, along with representatives of several member airports, participated on the ASAC Working Group on Airport Access Control in the development of substantive, meaningful, and risk-based recommendations. Further, the final report accurately recognizes that each airport is uniquely different and one size certainly does not fit all.

In addition, some have called on TSA to mandate that airports immediately implement 100 percent employee screening. As I will outline in my testimony, 100 percent employee screening does not translate to 100 percent security and moving forward with such a mandate is simply the wrong approach.

Although employee screening is one of the multiple layers in the aviation security system, it is not a stand-alone "solution" and should not be viewed as a "silver bullet," and I am in agreement with the risk-based approach identified by the ASAC.

In 2008, Jacksonville International Airport participated, along with other airports, in a Congressionally-mandated employee screening pilot program conducted by TSA. Despite augmented TSA Transportation Security Officer (TSO) staffing drawn from other airports to support 100 percent screening during the pilot program, there was a negative impact on checkpoint screening operations, and significant additional TSO staffing would have been necessary to permanently sustain 100 percent employee screening. Construction was also disrupted during the pilot and it became necessary to devote resources to screen the drivers and cement vehicles in a timely manner in order to prevent the cement from hardening before it could be delivered.

As occurs routinely at other small and medium-sized airports, employees regularly transit between public and sterile or public and secured areas. At large airports, hundreds of employees transit such areas during shift changes and at other times. Not surprisingly, it was observed during the pilot that the same employees were repeatedly subject to screening throughout the day.

During the 90-day employee screening pilot at Jacksonville International Airport, approximately 121,000 employees (51,000 of which were passengers in about 35,000 vehicles) were screened, but only one prohibited item was discovered.

The costs associated with the implementation of true 100 percent screening of employees at airports in the United States are staggering and are estimated to be in the tens of billions of dollars for the first year alone. Given the questionable security benefit of such a costly initiative, and in consideration for the significant impact on aviation operations, 100 percent employee screening is simply not realistic.

As the ASAC appropriately noted in its Final Report on Airport Access Control, there is no system domestically or internationally that "would qualify as 100 percent screening of 100 percent of all airport employees to passenger screening standards." Implementing such a system in the United States would necessitate a significant investment of resources that would then be unavailable to address other pressing threats.

A 2008 Homeland Security Studies and Analysis Institute (HSSAI) report—on the pilot program conducted at Jacksonville and other airports—titled, *Airport Employee Screening Pilot Program Analysis,* concluded that "a random screening strategy is the more cost-effective solution" for airports.

As identified by the ASAC, there is no perfect security system. The multiple layers of security—which can be routinely enhanced or modified—provide an effective means to secure passengers, employees, and facilities. A clear strength of this type of system is the unpredictable nature of the individual layers of security and the fact that many airport and aircraft operators exceed the baseline security requirements through the implementation of additional processes, procedures, and technologies that consider and are adapted to their unique geographic locations and facility designs.

Therefore, multiple layers of security, including enhanced background checks, security awareness training, and random screening of employees, as recommended by the ASAC, are much more effective than a rigid and predictable 100 percent employee screening regime.

RANDOM AND UNPREDICTABLE SCREENING

Unlike airport operators, TSA is in the business of effectively and efficiently screening passengers, baggage, and employees at airports. A key element of the TSA Playbook program, formerly known as the Aviation Direct Access Screening Program, is the roving teams of TSA Transportation Security Officers, Behavior Detection Officers, and Transportation Security Inspectors that conduct random and unpredictable physical screening of employees working in or accessing secured areas. The Playbook program has proven to be very effective in mitigating risk.

Some airports work in close partnership with TSA in support of Playbook operations to close certain access points and funnel employees through the screening locations. The Playbook program mitigates the risk of prohibited items being introduced at the perimeter, which would go undetected under a fixed-point employee screening system. In addition to introducing a high level of deterrence, Playbook provides employees the expectation of being screened at any time, not just when they enter through an access control point. This type of random and unpredictable screening program represents a formidable layer of security.

RISK-BASED, MULTI-LAYERED SECURITY

Several years ago, TSA appropriately identified the need to transition from a one-size-fits-all approach to risk-based, intelligence-driven initiatives that not only enhance security but also increase efficiency. With limited industry and Government resources, risk-based security programs—and regulations—are essential, as we simply cannot continue the process of adding new security requirements and deploying new technology to respond to each new threat.

Probably the most significant risk-based security initiative is TSA PreCheck, the agency's trusted traveler program, which provides expedited screening to travelers who are enrolled and pre-vetted while focusing the most invasive screening resources on those about whom the least is known. This type of risk-based system is absolutely what is needed and TSA should be commended for directing the implementation of this and other risk-based security initiatives.

We also need to commit to an on-going transition from the one-size-fits-all approach in the regulatory environment to risk-based security measures and regulation. With only limited resources available, it is essential that airports have the flexibility to apply security measures to those areas where they have the greatest ability to effectively reduce risk.

Airport security systems rely on multiple risk-based layers of security implemented in partnership with airports, airlines, and the TSA. While each layer is not designed to be impenetrable, the individual layers have the ability to deter and mitigate potential risks, and when integrated, the multiple layers provide a robust aviation security system that is not only effective but also capable of being readily adapted to address new and emerging threats.

Through the implementation of the risk-based enhancements identified by the ASAC, the current system will be even more effective in mitigating risk.

EMPLOYEE BACKGROUND SCREENING

An essential layer of security is the multi-faceted employee background screening process which is initiated prior to an employee being granted access to the secured area of an airport. In advance of issuing a Security Identification Display Area (SIDA) badge, which provides unescorted access privileges to secure areas, airport operators conduct extensive vetting of employee backgrounds. There are two critical facets of the employee background screening regime that all employees who work in secured areas must successfully pass: A fingerprint-based Criminal History Records Check (CHRC), and a Security Threat Assessment (STA). Upon receiving an application from an employee seeking unescorted access to a secured area, airport operators validate the identity of the individual, collect and transmit their fingerprints and the associated biographic information to the TSA. The biometric fingerprint data is routed by TSA to the FBI for a CHRC. Through the STA process, TSA conducts a threat assessment against terrorism and other Government databases.

If the STA reveals derogatory information about the individual, TSA informs the airport operator that they must not issue a SIDA badge granting unescorted access privileges. If at any point thereafter, recurrent STA vetting reveals derogatory information about an employee with unescorted access, TSA will notify the airport operator to immediately revoke their SIDA badge. Similarly, in accordance with existing regulations, when an airport operator discovers, during a review of CHRC results, that an applicant has been convicted of a disqualifying criminal offense within the previous 10 years from the date of application ("look-back period"), they refuse to issue the individual a SIDA badge. A distinct security feature is the ability for airport operators to review each and every applicant's criminal record to make a determination about their suitability for being granted unescorted access privileges.

Although some airports go above and beyond the baseline measures in current TSA regulations and have implemented longer "look-back periods" and/or an expanded list of disqualifying criminal offenses, others are unable to do so due to restrictive State laws. While some airport operators re-submit a portion of the population of SIDA-badged employees for a CHRC, it only provides a snapshot of their criminal record as of the date of submission.

As recommended by the ASAC, the "look-back period" should be extended, and, through collaboration between Government and industry, a harmonized list of disqualifying criminal offenses should be developed.

PERIMETER SECURITY

Airport perimeter security involves multiple layers of integrated processes, procedures, and technologies. Although there is no perfect perimeter security system, the multiple layers of security—which airports routinely enhance—provide an effective system to deter and detect potential intruders. While perimeter fencing and controlled access gates are the most outwardly visible layer of security, there are numerous other layers (systems), both conspicuous and inconspicuous, in place at airports to bolster perimeter security.

Frequent patrols of perimeters in the public and secured areas are conducted by airport and airline personnel, law enforcement officers and other representatives. In addition to patrols, employees at airports are trained to identify and immediately report suspicious activities.

Many airports go above and beyond the baseline security requirements for perimeter security, implementing additional processes, procedures, and technologies that integrate more effectively with their unique geographic locations and facility designs.

The individuals involved in most of the "breaches" in recent reports were promptly apprehended. Rather than presenting a gaping vulnerability as some would have us believe, this is clear evidence of the effectiveness of the layered security system in place at airports. In addition, none of the individuals have been linked to terrorism, and the suggestion that terrorists may attempt to breach perimeters is purely speculative and not based on any empirical data.

Airports, in conjunction with representatives of the TSA, the FBI, and other Federal, State, and local law enforcement officials, conduct joint vulnerability assessments (JVA) of their facilities, systems, and perimeters. The JVA results, along with the latest intelligence information, are used by airports to direct the application of resources to enhance individual security layers.

An investment in research and development (R&D) of promising perimeter security technology is essential. In order to evaluate the effectiveness in the operational environment, TSA should commission a pilot test at airports of promising technologies identified through the R&D process. These pilot programs would provide valuable information about cutting-edge technologies that could be used to by airports to further enhance perimeter security.

The National Safe Skies Alliance, in partnership with airports, and funded through the Airport Improvement Program, conducts testing and operational evaluations of security technologies designed to further enhance perimeter security and access control. Many airports have deployed the systems tested and evaluated by the National Safe Skies Alliance. The reports, which are available to all airports, provide specific details about the application and functionality of technologies tested under the program and contain valuable information for airports as they make decisions on which technologies may work best at their facility.

BIOMETRICS

Although biometric access control technology can be a potentially useful tool in limiting access or supporting post-incident forensic analysis, such systems are not a panacea and would not have prevented the situation involving the unauthorized transportation of guns on-board aircraft. In addition to being incredibly costly and challenging to integrate with some legacy airport systems, biometric access control systems are susceptible to environmental conditions and contamination from substances routinely found in the aviation industry. Reports from TSA officials subsequent to a study of biometrics in aviation and other sectors revealed that such systems are not ready for full-scale deployment at airports, and individual airports should conduct a cost-benefit analysis to determine whether to procure and deploy such systems.

LOST BADGES

Recent reports about lost and unaccounted SIDA badges failed to accurately characterize the situation and provided no information about the various security processes, procedures, and technology specifically designed to mitigate potential vulnerabilities. Many airports go above and beyond TSA regulations and have designed additional features into their SIDA badges and access control systems to address concerns with lost or unaccounted badges. These include requirements for not only a swipe of the badge but also a personal identification number or a biometric to gain access through controlled portals, security features incorporated into the badges, and employee training. Some airports have deployed closed circuit television at access portals. In addition, airports frequently re-issue badges to all authorized employees. Upon receiving reports from badge holders of lost or stolen identification media, airports immediately deactivate the badges in their systems. Due to their sensitive nature, other security features incorporated into access control systems cannot be discussed publically.

SECURITY DIRECTIVES VS. PROPOSED AIRPORT SECURITY PROGRAM CHANGES

The most effective approach to rulemaking exists when regulatory agencies afford airports the opportunity to comment on proposed changes to their airport security program. Over the years, ACI–NA and airports have participated on various National and international Government/industry working groups intended to enhance aviation security as well as improve efficiency. This coordinated process has been very effective in allowing TSA to identify potential threats to civil aviation, and industry to collaboratively develop aviation security enhancements that minimize unnecessary costs and operational impacts at airports.

Although TSA has the ability to avoid the notice and comment process and issue security directives (SDs), this regulatory option should be strictly reserved for situations involving an immediate threat, as was stipulated in the Aviation and Transportation Security Act and current TSA security regulations. Airports do not believe that Congress intended to provide TSA such latitude that it could issue SDs absent or months after an identified threat.

SECURITY ENHANCEMENTS

Following are five suggestions to further enhance the security of airport access control:

1. Invest in Intelligence

The importance of timely and actionable intelligence information being used to disrupt terrorist plotting and adjust security baselines cannot be emphasized enough. In the aviation industry, history has demonstrated that effective intelligence information and sharing plays a critical role and provides one of the best opportunities to identify potential threats and prevent terrorist attacks. By way of example, the 2006 liquid explosives plot, the 2010 toner cartridge bomb plot and, more recently, the 2012 "improved" underwear bomb plot were all foiled by intelligence information developed and provided to industry by intelligence agencies.

Armed with this type of information, airports make adjustments to security measures to mitigate threats. Therefore, it is crucial to invest in and provide additional resources to the intelligence agencies with the understanding that actionable intelligence information be shared with airports and airlines in a timely manner.

2. Review and Revise Security Requirements

Even today, there continues to be general hesitancy or fear of rescinding long-standing security requirements, even when it is readily acknowledged that they are outdated—because no one wants to be accused of being weak on security. However, it is the very essence of risk-based security to continually assess the latest intelligence information and conduct informed reviews of security procedures. Based on such a review, adjustments can be made so security measures maximize risk reduction, something that may necessitate shifting or reallocating security resources to bolster other areas. This reallocation of limited resources ensures that they are being applied to those areas where they can most effectively reduce risk.

3. Institute Real-Time Recurrent Background Checks

Unlike the STA process, through which TSA conducts perpetual vetting of employees who have been granted unescorted access privileges, the CHRC is currently a one-time snapshot of the applicants' criminal history. According to the FBI, Rap Back provides "the ability to receive on-going status notifications of any criminal history reported on individuals holding positions of trust." When implemented, this program will provide airports (and airlines) much better and needed visibility into employees' criminal records, allow them to make informed determinations as to the suitability of existing employees and greatly assist in making determinations about whether employees should be allowed to retain their unescorted SIDA access privileges.

As recommended by the ASAC, TSA should ensure the immediate implementation of the FBI's Rap Back program, so that real-time recurrent CHRCs are conducted on SIDA badge holders.

4. Expand Random Employee Screening Operations

As a means to enhance an important layer of security, TSA should further expand its Playbook employee screening program, so that every employee entering or working in a secured area of an airport has the expectation that they will be subject to screening. Airport operators can support expanded Playbook operations by selectively closing access portals in order to route employees through the screening locations.

5. Institute an Airport Security-Focused Grant Program

Although DHS, through its Homeland Security Grant Program, dispenses billions of dollars annually for systems and technology to bolster State, Tribal, and local preparedness, resiliency, and improve security, very little, if any, is allocated to airport operators. As airport operators have only limited funding that must be prioritized across a multitude of safety, security, and operational projects, an airport security-focused grant program would provide readily available funding to support perimeter, access control, and other security enhancements.

CONCLUSION

Jacksonville International Airport and airports across the United States are committed to working with Congress, TSA, FBI, CBP, State, and local law enforcement agencies and aviation stakeholders to enhance airport security through the application of risk-based measures. The recommendations identified by the ASAC for multi-layered, risk-based security enhancements provide the best approach to further enhance the security of the aviation system.

Working in coordination with ACI–NA and airports, TSA should make it a priority to move forward with the implementation of the ASAC recommendations to enhance airport security. Through continued Government-industry collaboration to enhance security, we can better achieve our mutual goals of enhancing security and efficiency while minimizing unnecessary operational impacts.

Thank you for the opportunity to submit this written testimony.

Mr. KATKO. Thank you very much, Mr. Grossman.

I will start with both of you. One of the five programs that Homeland Security has recently implemented through Mr. Johnson was the requirement that airports reduce the number of access points to secured areas to an operational minimum. Sounds good. What does that mean to you?

Mr. GROSSMAN. Ladies first.

Ms. OLIVIER. Each airport needs to work with their local TSA on that and with all of their tenants. The layouts of the airports, of course, as you know, are very different. You can have cargo areas, you can have direct terminal areas, you may have general aviation areas. Depending on the layout of the airport, there may be a need for various more remote access points, as well as ones that are close to the terminal.

So in reducing those, an airport has to understand what the necessary movements are through these areas, as well as take into consideration what the vulnerabilities and risks associated with that location are. In heavily-trafficked airports, you have to understand what it does to the daily operations of the airport. Often in cargo situations it is very time-sensitive and so deliveries have to be made very quickly. They have to get in and get out and on their way. So we have to understand for every portal that we might reduce what the implications of that are.

Mr. KATKO. Mr. Grossman.

Mr. GROSSMAN. Over the last several years at Jacksonville, we have reduced our entry points from 24 to 14. During the pilot program that we participated in, that number was reduced to four. That became an operational nightmare, both for airport personnel and, more importantly, for airline personnel.

So there is a right answer. For every airport it is going to be different. I think with all of the new security measures, airports do need to take a second look at that: How are we going to control those access points and work with the TSA so that the random screening is effective at each and every one of those entry points?

Mr. KATKO. Who decides what is an adequate reduction in entry points? Who says, "That is good, you are where we want you to be"? Or who decides?

Ms. OLIVIER. We think it should be consensus. At an airport, we engage the entire airport in the security program of the airport. Together, we try to get a comprehensive problem solving from all of our partners. That includes the TSA. It includes our tenants. We invoke our employees through committees to evoke their best ideas. So together with some very deliberate time and motion studies and the like, we come to an informed decision about what, in fact, can practically be decreased.

Mr. Grossman is quite correct, airports across the country have already worked in previous rounds to reduce the number of access points. As we all continue to work on our airports and oftentimes as construction changes on the airports, that will present other opportunities for us to do further work in that area.

Mr. GROSSMAN. Yeah, Mr. Chairman, as you know, all airports are required to have airport security programs that are put together by the airport and approved by the TSA. We do that in conjunction with all of our partners.

One of the things that is most impressive is at many of our airports, if not most of our airports, the cooperative working relationship between the TSA, the airport, and the airlines. I will tell you, it has not always been that way. But I think in the last few years we have worked very well together to solve problems that not only enhance security, but work operationally for the airport.

Mr. KATKO. So is it fair to say that the ultimate arbiter really is TSA through your airport security plans that you present them?

Mr. GROSSMAN. I would say yes.

Mr. KATKO. Okay. Now, have either one of you begun that evaluation given the recent guidelines from Homeland Security?

Ms. OLIVIER. Personally in our airports, sir?

Mr. KATKO. Yes.

Ms. OLIVIER. Yes, sir. We continue to look into that.

Mr. KATKO. Okay. When you say "we," to whom are you referring?

Ms. OLIVIER. Well, I have several airports that I work with.

Mr. KATKO. Yes, you do.

Ms. OLIVIER. So we address this at things like our security consortiums with our partners, but I also have the airport security managers at each of those airports looking at opportunities to how we can reduce these gates. In fact, we are looking at that right now at JFK.

Mr. KATKO. Okay.

Mr. GROSSMAN. I think in almost all aspects of these recommendations we are a bit ahead of the game. We have reduced portals at our airport with regard to airport employees. An employee who gets on an airplane to take a flight without going through security is terminated as soon as that is discovered. There is no tolerance.

In many of these other areas, we conduct with airport personnel over 250 temporary checkpoints every month at access doors with our staff. We have beefed up all of the challenge programs in the secure area. So just even talking this morning with the staff about the new security directives that are out, we were talking about: Okay, when does Rap Back come about?

Because we already do additional background work every year when we review badges through a law enforcement database called LexisNexis. So we check that. We basically go back when we do the initial background check, and this is different in every State depending on State law, but we go back to when the person was 18 years old, regardless of how old they are now.

Mr. KATKO. That is great. That is great.

Mr. GROSSMAN. We will evaluate acts that happened back many years ago to see if there is a pattern and use our judgment as to whether or not that person should have a security badge. So it is basically a daily thing.

Mr. KATKO. One of the things that we are probably most concerned with, and you have heard this already several times today, is that point when the employee goes from the nonsecure to the secure area. How do you best try and prevent that from happening? I have heard a lot about the risk-based theories and the randomization and everything, which I understand on both sides, both before and after they get into the airport secure area.

But at that critical point we might be able to stop it. It is probably where the committee itself is really kind-of hung up the most. I would like to hear from both of you. What do you think with the minimum requirements for a security check, or however you want to say it, for the access points when you are going from the nonsecure to the secure area for employees?

I guess, for each of you, in your own words, tell me what you think should be the minimum requirements for each of the entry points.

Mr. GROSSMAN. I think in general I would say, if we were doing it, it would be a security person or two, minimum be able to wand somebody, make sure they are not carrying a gun, and then a fairly detailed inspection of anything they were carrying. I think if TSA is doing it, they have a bit more access and training to check for explosive residue than we do. We are just unequipped to do that. So I think it is going to be a combination of both TSA personnel, and at airports that can do it, airport personnel.

Mr. KATKO. So is this for each and every entry point for employees?

Mr. GROSSMAN. In doing it on a random basis, absolutely.

Mr. KATKO. Okay. So when you say on a random basis, okay, what does that mean? So sometimes they are there and sometimes they are not?

Mr. GROSSMAN. Correct.

Mr. KATKO. Okay. All right. So you would have that randomization component, which I understand you all do anyways, you all support, but I am talking about the physical composition, if you will, of what that entry point looks like. Tell me what you think it should look like.

Ms. OLIVIER. Well, I would express some level of caution. I may be misinterpreting your question, but I would be reluctant to impose a particular specific model or requirement on a particular portal, because portals have different functions, they are trafficked by different people, they are located in different places.

I would be reluctant to impose a solution that is uniform. I guess specific to that is, I would be reluctant to impose a uniform solution for all portals because that can then militate against the flexibility and agility that is needed at airports to address the various security postures that they need to employ depending on their information about risk and threat, et cetera.

The minimum requirement certainly is that the people conducting the inspections, or physical searches, are trained to do so.

Mr. KATKO. Let me back up, though. You see, we are getting again into the randomization aspect of it, and I am talking about just the physical description. I know I probably am sounding like I am too focused on it, but we still don't have it yet. I mean, doors should be locked. They have a SIDA access badge. For the ones that aren't manned, what should be there? Ones that are manned, what should be there? That type of stuff. The nuts and bolts.

Mr. GROSSMAN. I mean, I would suggest, as is done now at many airports, just swiping a badge isn't enough. There has to be some form of other means that you have to enter in. It could be biometric, it could be your own personal code, et cetera. That is as a minimum. The door absolutely has to be locked.

Mr. KATKO. We are getting somewhere.

Ms. OLIVIER. Well, certainly. Or guarded.

Mr. GROSSMAN. Right.

Ms. OLIVIER. There may be times when you have to have the door open.

Mr. GROSSMAN. When a door malfunctions we automatically put a guard on the door.

Mr. KATKO. Right.

Mr. GROSSMAN. So I guess there are probably things we take for granted, of course, because we live it every day.

Mr. KATKO. Right. Right.

Mr. GROSSMAN. But I do think that those things are important. Then it is really going to be what is decided about what is the random check process going to look like.

Mr. KATKO. Right.

Mr. GROSSMAN. No door should ever be left unlocked.

Mr. KATKO. Okay. So as far as the random check process goes, we are trying to figure out how to get some sort of prescription to this without causing too much problems for the airports given their operational flexibility. But we are concerned about having some sort of basic standards that everyone understands they have to adhere to, and obviously to randomness.

Much of what the ASAC says is great, but it still doesn't say how often it should be done or when it should be done or how often. People like me facing this random screening, is it once a month? Is it once a year? Is it 1 out of 4 employees on a daily basis should get screened?

I mean, I guess, we want to set achievable goals that they can abide by so when you come later on and do inspections of airports, and they say, you have only been screening 1 out of 1,000 employees, that is unacceptable. Without some sort of standards, your response could be: Well, that is what we thought was good for this airport, you know what I mean? So we have got to kind-of find a happy medium here.

Ms. OLIVIER. Basically, I think another way of saying that is what employees say to me all the time too is, how do you actually operationalize this, right?

Mr. KATKO. Correct.

Ms. OLIVIER. So I think further work, as you suggested, is going to be needed for us to work with our partners on that. But the ASAC did lay out some very fundamental principles for us to build upon on that. In the recommendations, it did suggest that there needed to be a reasonable expectation on the part of employees that they would be checked and inspected that moment when they walked through that portal.

So whatever methodology we construct, whatever methods, whatever channeling we construct, is that employees have to expect whenever they come to work that day or whenever they return from lunch that they have a reasonable expectation that somebody is going to be taking a look at what they are carrying.

Then to pick on an area in the ASAC recommendations that may have come across a bit obscurely is that we believe that the particular frequency, where we do it, when we do it, would be a matter of rather smart modeling, and this is where you and I are going to have some statistic lessons after class.

Mr. KATKO. Oh, man. I am getting flashbacks of my days at Catholic schools with the nuns. So go ahead.

Ms. OLIVIER. Yeah, but I am not carrying a ruler.

Mr. KATKO. That is right. Thank God.

Ms. OLIVIER. So, in fact, we will be able to work with industry experts in this area to determine the most efficacious model for each area where we can achieve that ultimate result that everyone has the reasonable expectation, it is very real, and it achieves a level of frequency and stratification that the public too feels that we have a very good chance of identifying any problems as they emerge.

Mr. KATKO. Mr. Grossman.

Mr. GROSSMAN. Yeah, I think the answer is much more frequently than once a month. It may not be every day, but it would be multiple times each month.

Further, it needs to apply to everybody. In the pilot program, a number of employee groups were exempted from it, most particularly TSA employees, who probably access back and forth more times each day than any other group of employees at the airport.

So that is going to be a big challenge as to how we get those people through these temporary checkpoints, but it has got to be done.

Ms. OLIVIER. Remember too, when he described temporary checkpoints, exactly that. Sometimes we can choose to close down a checkpoint, right, or choose to close down a portal and say every employee or the next 10 employees have to go over to this other area where we do have screening set up, right? So there are many different options to achieve this.

Mr. KATKO. Right. Okay.

I think I have got it, and it is just going to take some more fleshing out. But the overarching observation is that we all agree we have to step it up, and just a question of how to do that and how to make sure that the people that are committed to it are doing it the same way that people who may not have the same desires to.

My concern is not so much an airport, you two, because you sound like you are on your game, but what about an airport authority that is really struggling for money? There are pressures from whomever and maybe they cut corners. That is why there have got to be some sort of generalized standards, minimal standards, which must be uniform so at least when they fall below those minimum standards we can do something about it. Right?

Ms. OLIVIER. May I interject a comment that I don't think anybody expected to be saying?

Mr. KATKO. Sure. Of course.

Ms. OLIVIER. But I would like to assert that many security professionals through the commercial airports in this country talk to one another. We do it through usually two associations, ACI and AAAE, and many of us are members of both. We have committee work. We have ways of corresponding in many other ways. I can attest that every day these folks are talking to one another by email, phone call or what about particular issues they are trying to solve at their airport and how they can address it.

That involves people in the smaller airports that you have just cited, as well as the larger airports. There is a lot of cross-fertilization, everyone committed to trying to find solutions, things that others have thought of that we can capitalize on. My colleagues and I steal any good idea we can find.

Mr. KATKO. That is a good thing. Collaboration is wonderful.

Now, I want to switch gears if I can and talk about some of the other subject areas, which I think we are all pretty much on agreement on these, that is the vetting of the employee and security threat assessment. The information set forth in the ASAC report about this subject, do either one of you have any questions or objections about those?

Mr. GROSSMAN. No, I think we are doing more than that right now. So we will continue to do that, but I think that process can be further assisted using the FBI's Rap Back program.

Ms. OLIVIER. Yes, and taking a look, people need to take a look at this, but perhaps expanding the disqualifying crimes, expanding the length of look-back, integrating with certain foreign databases for a better understanding in that way. All of those recommendations we fully support.

Mr. KATKO. Okay. All right. As far as the internal controls and auditing of airport-issued credentials, I presume neither one of you have any questions about that. I mean, when people are losing their credentials, that is a problem?

Mr. GROSSMAN. Right.

Ms. OLIVIER. Sure.

Mr. KATKO. Yeah. Okay. As far as the risk-based security for higher-risk populations and intelligence, I want to talk a bit about that. What do you understand that to mean, and what do you think about what the ASAC's recommendations are about that?

Mr. GROSSMAN. Well, I think I have always said that, unfortunately, over many decades as an industry we have been very reactive. We seem to plan for yesterday's incident.

Mr. KATKO. That is what we are doing right now, I guess, in a way. We want to get better than that.

Mr. GROSSMAN. Right.

Mr. KATKO. Right.

Mr. GROSSMAN. We are starting to get more proactive, developing scenarios of what might happen and what do we do, how do we prevent it? But the real key is intelligence. As I mentioned in my testimony, if there are more resources available, give them to the FBI, give them to other agencies developing real intelligence, and then let's do a better job of, No. 1, stopping these acts, and sharing the information locally.

I think the Federal agencies are doing much better at talking to each other. They still have a ways to go in talking to us. That will come over time. But really, we have to stop bad actors before they get to the airport, when you are talking about terrorists.

Mr. KATKO. I agree with that.

Ms. OLIVIER. I would like to highlight something too. We do often struggle to try to understand what intelligence is out there that can affect our day-to-day decisions at the airport, but also our long-term decisions. What intelligence out there can help me decide on major investments at the airport for protective elements, perimeter intrusion detection, surveillance systems, bollards on the frontage of airports.

Those kinds of major capital investments may be worthwhile, but I need to know from an intelligence standpoint, is that appropriate or is there intelligence out there that tells me I should change some of my operational procedures or policies?

There is an activity initiated by the Department of Homeland Security right now on intelligence that is attempting to reach out to industry partners, airlines as well as airport operators, to participate in an effort, referred to as ADIIC, to understand what intelligence is actually useful to airports.

So I think that is a very excellent new initiative to bring airports closer to this intelligence-gathering effort and to ask airports: Is this useful to you? What else would you like to know? So I think that is very promising.

Mr. KATKO. Okay. Last, and then I am just going to bounce something off both of you, security awareness and vigilance. I take it you all agree that the efforts to beef that up and establish a hotline, if you will, and to encourage people to speak up when they have concerns is fine with both of you.

Mr. GROSSMAN. I think it is fine. I have always been very impressed with how serious airport workers take their role in security. We drill it into them when they first come on as an employee, whether it is my employee or an airline employee, and every year they get recurrent training that they are part of the security program. I think it works very effectively.

The tools that were advocated in the report are all good enhancements to that. But I think they do a pretty good job right now.

Mr. KATKO. Now, the last thing I will leave you both with before we wrap up, and that is, as we were sitting here I was thinking how do we kind of ensure that this organic exchange of information and information sharing and just kind-of institutionalizing the information sharing on the security side for employees as well, how do we do that moving forward?

I just want to bounce this off of you. What would your thoughts be about using ASAC as a vehicle through which maybe on an annual basis you kind-of do a review of what you have learned for the year, basically, and recommendations going forward, so all airports can have it, and we can have it, and if there are things we need, if we need to get more money to you, if we need to do things differently, if we need to tweak the laws, we need to back off on this, we have kind of a uniform way to do that? I think it just would lead to a better dialogue on both sides of the fence. What do you think about that?

Mr. GROSSMAN. As an outsider to the ASAC process, I will tell you how impressed I was that it really represents almost the first real collaboration of industry and TSA. I think the results of that were shown in how the report was received. They did a great job. I think if you can institutionalize it and make it part of the culture, I think that has been one of the issues we see with TSA, is what is the culture, and it needs to be a culture of collaboration. Because most at TSA headquarters have never run an airport. They have never worked at an airport. They need our input. This was a prime example of what can come from getting that input.

Ms. OLIVIER. It was a very respectful process. It provided for a great deal of crosstalk across the industry. Remember that it is not just airports that are responsible for many of the things that were discussed today, but our airline partners, a great deal of responsibility there.

Mr. KATKO. Correct.

Ms. OLIVIER. To bring all the parties to the table with the TSA for joint problem solving certainly seems to reap the highest level of product and benefit in a very short length of time.

So we feel that this kind of collaborative process is a lot better too than issuing perhaps certain directives that haven't been vetted in the same way.

Mr. KATKO. Understood. Understood. Give me one moment, please.

Unless there is anything else you want to offer here, I appreciate the efforts. Again, I will reiterate what I said to Mr. Carraway. This type of collaborative effort on attacking a real problem is what we are supposed to all be doing. I am proud to be part of the process. I very much appreciate your efforts in that regard as well.

Moving forward we have got to remember, we are all trying do the same thing here. There are not two sides to this fence. We are all in the same boat. We look at it from different perspectives, and that is a good thing.

So moving forward, I hope we continue this collaborative relationship on this issue and others relating to the airline industry. The risks are far too great to do anything other than that. I just wish more Americans would see that sometimes we can work together and get things done. I think this is a good example of that.

So thank you both very much, and have a good evening.

Ms. OLIVIER. Thank you, sir.

Mr. GROSSMAN. Thank you very much.

[Whereupon, at 4:20 p.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FROM CHAIRMAN JOHN KATKO FOR MELVIN J. CARRAWAY

Question 1a. At the hearing, you announced that TSA is requiring airports to increase aviation employee screening to include additional randomization screening throughout the workday.

What is the estimated percentage of airport and airline employees being screened at Federalized airports daily?

Question 1b. Will airports be required to screen a minimum percentage of employees on a daily basis? If so, what methodology did TSA use to determine that percentage? Do you think such measures are sufficient in providing employees with the expectation that they will be subject to screening every day?

Question 1c. Has TSA issued minimum screening standards for airports when conducting employee screening? If so, please describe those standards.

Question 1d. In your opinion, what are the best and most effective options for access points to ensure the integrity of the security apparatus?

Answer. The Transportation Security Administration (TSA) captures general metrics associated with employee screening operations conducted by TSA; however, it does not maintain metrics identifying the percentage of airport employees screened as they enter the sterile area. TSA is using a risk-based security approach to affect the increase in employee screening, which includes TSA-directed inspections conducted by the airport operator, as well as TSA-conducted screening. TSA-conducted screening includes screening of airport and air carrier employees at TSA screening checkpoints (as required for sterile area airport tenants), as well as at other access points in the Aircraft Operations Area (AOA), sterile, secured, and cargo areas.

Airport operators are required to conduct random inspections of individuals entering the sterile area at entry points other than the screening checkpoints to verify that they have appropriate and valid identification and access control media, and to determine if they are carrying prohibited items other than those required for operational needs. The inspections must be clearly visible to other individuals exercising their access privileges. While TSA does not require that a specific minimum percentage of employees be inspected, the rate and locations of random inspections must be approved by the Federal Security Director and must be frequent enough such that there is a reasonable expectation that individuals exercising their unescorted access privileges will be subject to an inspection. Additionally, TSA does not issue Standard Operating Procedures (SOP)-type parameters to airport operators, rather their requirement is to verify access authority and determine if an individual is in possession of prohibited items. In response to direction from Secretary Johnson to address insider threat vulnerabilities at domestic airports, TSA recently issued an Information Circular (IC) to airport operators encouraging them to work with their Federal Security Directors (FSDs) to utilize a continuous random methodology of inspections; increase the breadth of inspections to include public to secured area access points in addition to public to sterile area access points; and capture the updated measures in their regulated Airport Security Program (ASP) so that the measure become enforceable, rather than a recommendation through IC. TSA currently is compiling a survey establishing the level of the cooperative compliance with the IC recommendations. Industry has been advised by TSA that if there is insufficient voluntary process with the measure contained within the IC, TSA will consider other mandatory means of compliance. Airport operators are also expected to collaborate with their FSDs to determine the best location, frequency, and duration of these random inspections and amend their security programs accordingly. In addition, TSA also conducts screening, via Playbook, of individuals entering the sterile and secured areas of airports at access points other than the screening checkpoint on a random basis.

The combination of enhanced vetting, security awareness training, intelligence and information sharing, and random screening/inspection help to ensure that airport employees do not introduce prohibited items into the sterile area or secured area. Prohibited items may go undetected if airport employees undergo only a fixed point-of-entry inspection process. Introducing a high level of random and unpredictable screening/inspection presents a formidable deterrence. As noted above, each airport operator works with its FSD to establish the manner and frequency with which these measures will be implemented and that activity is supplemented by TSA screening operations.

Question 2. On average, how many Playbook operations are run daily and how many employees are screened in a typical day? Does TSA intend to expand Playbook operations so that more randomized screening occurs?

Answer. Playbook is regularly performed at 117 of our Nation's busiest airports, which have been identified as higher-risk locations. Currently, Playbook is required at 100 percent of CAT X and I airports, in addition to 40 percent of CAT II airports. Other airports have the ability to implement Playbook, as needed. On average, across the 117 Playbook-required airports, the Transportation Security Administration (TSA) conducts approximately 5,000 operational hours of Playbook per day, focusing approximately 95 percent of these hours on employee screening. As a result, Playbook screens about 45,000 airport employees daily. These figures have steadily increased over the past few months as TSA has expanded operations to concentrate more on employee screening.

Question 3a. How does TSA define "operational minimum" as the term pertains to the number of access points to secured areas of an airport?

Does TSA believe it is best to let local Federal Security Directors and airport officials determine the operational minimum for the number of access points?

Question 3b. Do you think there should there be a National definition?

Answer. The Transportation Security Administration (TSA) has not provided a numerical value to the term "operational minimum." Each airport has unique operational and geographical considerations that must factor into the decision as to how many access points are appropriate to achieve an operational minimum. Accordingly, based on operational and geographical diversity of airports, varying in size from the Los Angeles International Airport to Tupelo Regional Airport, a Nationally-driven numeric value is not feasible. For that reason, there is no definition for operational minimum, and TSA currently does not plan to create one.

TSA believes that the Federal Security Director (FSD) at each airport, working in coordination with airport officials, is in the best position to determine the operational minimum number of access points for that airport.

TSA has directed FSDs to work with airport operators to further review the minimum number of access points to ensure they are at the operational minimum, and to include that information in the airport's Airport Security Programs.

Question 4. The Aviation Security Advisory Committee recommended updating the list of disqualifying criminal offenses for SIDA badge holders. What criminal offenses do you think should be added or removed from the list?

Answer. See response, Question 5.

Question 5. In your testimony, you stated that individuals who have committed a statutorily-defined disqualifying offense within the preceding 10 years are not eligible for a SIDA badge. Do you think the 10-year look back period is adequate? How feasible is to look back to age 18 for disqualifying offenses?

Answer. TSA will require additional time to review the current list of disqualifying crimes and any new criminal offenses that should be considered to disqualify individuals from receiving a SIDA badge. Additionally, TSA will need more time to evaluate the 10-year look-back period to consider whether changes are warranted. Any updates to the list of disqualifying offenses or the length of the look-back period will likely require legislative and rule-making changes.

Question 6a. Is TSA considering creating a National database for airport employees?

Could it be modeled after the Federal Aviation Administration's database of individuals who hold some type of certificate (pilots, mechanics, etc.)?

Question 6b. How quickly could such a database be created?

Answer. TSA has a database of all airport employees for whom TSA has completed a security threat assessment (STA). TSA's system contains the biographic information these workers submitted to TSA as part of their STA and application for an airport credential which if approved, would afford access to airport secured areas. TSA is reviewing technical, regulatory, civil rights and civil liberties, and privacy issues related to implementing a National database that would be used for other purposes or accessed by other entities. When TSA has determined what, if any, legal or operational impediments exist, we can determine how long implementation would take.

Question 7. Is TSA creating a National anonymous tip line for employees to report suspicious behaviors? If so, what is the time frame for doing so? Which office would be responsible for investigating the complaints?

Answer. Yes, the Transportation Security Administration (TSA) has created a National anonymous tip line for employees to report suspicious behavior.

The anonymous tip line, 844–MY–ARPRT (844–692–7778), began operation on May 26, 2015, when materials about the tip line were delivered to the airports.

The Tip Line is routed to the TSA's Call Center. The caller will be informed that he/she has reached the TSA Call Center. Once the caller presses "2" to report a security threat, the call is then forwarded to the Watch Desk at the TSA's Transportation Security Operations Center (TSOC). The Watch Desk is staffed 24×7.

TSOC will refer the information to the appropriate office for further investigation.

Questions From Chairman John Katko for Jeanne M. Olivier

Question 1. What is the feasibility of mandating a percentage of airport employees that must be randomly screened daily at airport access points? If feasible, what do you think that percentage should be?

Answer. Mandating a fixed percentage of airport employees to be screened would limit the Transportation Security Administration's (TSA) and airport operators' ability to implement a risk-based and random screening methodology. A cornerstone of risk-based security is the continuous reevaluation of processes and protection measures in light of changing vulnerabilities, better understanding of risks, availability of new technologies, and the evolution of industry business practices. TSA and airport operators need the flexibility and agility to respond to not only changing operational needs but also changing threats and vulnerabilities—which would be hampered by a mandated percentage for employee screening. Rather, the ASAC working group recommends establishing a science-based methodology to determine "randomness" in the context of employee screening at airport access points.

It is critical from a security and resource perspective that risk mitigation efforts remain intelligence-driven, balanced, and effective. In a world of limited resources, we are concerned that placing so much emphasis on one approach—such as screening a certain percentage of employees—could divert significant funding from other critical security functions that are currently producing significant benefits.

Question 2. Is there an industry definition of "operational minimum" as the term pertains to access points for employees at airports? If so, what is that definition?

Answer. There is not an industry definition of "operational minimum." It is defined on a facility-by-facility, and often even terminal-by-terminal, basis in conjunction with air carriers, tenants, and TSA. Under current regulation, airport operators have already worked to reduce access points to an operational minimum and also segment which employee populations can use certain access points and when. Airport operators must also factor safety concerns into the determination of "operational minimum," often needing to keep access points active to meet fire code regulations and provide access or egress for emergency response. Condition changes, such as terminal modifications and flight schedule changes, may also provide opportunities for further reduction of access points. As a result, airport operators continuously monitor the need and utilization of each access point.

Question 3. In your opinion, what are the best and most effective options for each access point to ensure the integrity of the security apparatus?

Should there be a minimum threshold of technology (i.e. biometrics, CCTV) and physical screening?

Answer. Each access point should have the security apparatus needed to provide an agile screening response based on intelligence and a risk-based methodology that would result in all airport employees having the expectation of being screened. We would be reluctant to impose a specific requirement or standard for access portals because of the different uses, layouts, and populations using each of the access points.

Again, risk-based security provides for the continuous reevaluation of processes and protection measures in light of changing vulnerabilities, better understanding of risks, availability of new technologies, and the evolution of industry business practices. TSA and airport operators need the flexibility and agility to respond to not only changing operational needs but also changing threats and vulnerabilities—which would be severely hampered by a mandated minimum threshold of technology at each and every access point. Security resources, whether measured in terms of infrastructure or personnel, provide a higher degree of risk mitigation when used in random and unpredictable ways, consistent with risk-based security. Static security measures, such as physical screening done at the same place at the same time with the same technology, can be studied, tested, and more easily circumvented than those that are dynamic and less predictable. No single measure can provide broad-spectrum protection against risks or adversaries. Therefore, risk-based, multilayered security offers the greatest ability to mitigate risks through the application of flexible and unpredictable measures to protect commercial aviation. This also creates the expectation for airport employees that they can be screened at any time and any place.

Once again, it is critical from a security and resource perspective that risk mitigation efforts remain intelligence-driven, balanced, and effective. In a world of limited resources, we are concerned that placing so much emphasis on one approach—such as screening a certain percentage of employees—could divert significant funding from other critical security functions that are currently producing significant benefits.

Question 4. The Aviation Security Advisory Committee recommended updating the list of disqualifying criminal offenses for SIDA badge holders. What criminal offenses do you think should be added or removed from the list?

Answer. A comprehensive review of the list of disqualifying crimes is needed in order to adequately answer this question. The review of disqualifying criminal offenses should be done in the context of determining that an individual can be trusted to perform his or her job and responsibilities in a manner that poses no threat of intentional harm to themselves or others while in the secure areas of airports with access to aircraft. The review should ensure that the existing list of disqualifying criminal offenses is comprehensive enough to address the current threat environment and to address changes within today's legal system. Specific areas of review should include making a distinction between a charge and a conviction (since many serious crimes are plead down to non-disqualifying convictions), identifying patterns of misdemeanors or other non-disqualifying criminal offenses, and expanding the limited look-back period and variances in look-backs from the date of application instead of the sentence-release date, and increasing the potential for permanent disqualifying criminal offenses. The disqualifying criminal offenses should also be referenced against other similar programs operated by DHS, U.S. Customs and Border Protection, United States Postal Service, and Department of Transportation.

By regulation, airport operators are responsible for adjudication of the criminal history records check, which allows airport operators to know more about individuals that have access to their facilities. It is critical that airport operators maintain the responsibility for reviewing each and every applicant's criminal record prior to making a determination about their suitability for being granted unescorted access privileges. For example, in some cases, an individual is eligible under the list of disqualifying criminal offenses; however, the individual may require further scrutiny or at least situational awareness for the Airport Security Coordinator. In addition, some airport operators have adopted local regulations/ordinances and used other practices to add disqualifying crimes beyond those listed in the Federal regulation. TSA published *Legal Guidance on Criminal History Records Checks* (dated May 28, 2004) that states, "In addition to the disqualifying offenses set forth in the CHRC statute and regulations, a credentialing authority may apply its own criteria in making a decision to grant or deny unescorted access authority." Consequently, airports have added various processes to enhance their vetting practices. It would be helpful for airport operators to have the regulatory support for suspending or revoking access privileges if a current badgeholder is arrested for a disqualifying or serious crime.

Question 5a. In your opinion, are there any impediments to creating a National database for airport employees?

Do you think it could it be modeled after FAA's database of individuals that hold some type of certificate (pilots, mechanics, etc.)?

Question 5b. How quickly do you think it could it be created?

Answer. Given the transitory nature of aviation workers, a National database—maintained by TSA but available to all airport operators—of employees who have had their SIDA badges revoked would provide yet another security enhancement. Such a database would eliminate the potential for an employee whose unescorted access privileges were revoked because of security violations at one airport from transferring to another airport and being granted unescorted access privileges. This models best practices in other industries that maintain databases of sensitive information for reference purposes and suitability concerns.

The relevant information is already reported by airport operators to TSA which should facilitate a relatively quick creation of such a database. The biggest obstacles to implementation are likely addressing privacy and legal concerns on behalf of airport employees, providing airport operators access to such a database (which is key to its value), determining exactly what information will be included in the database (revoked badges, badges not issued, etc.), establishing a redress process for airport employees and allocating TSA resources for the database creation.

Question 6. Do you think the Aviation Security Advisory Committee (ASAC) should produce an annual report on airport access control security and employee screening?

Answer. As we stated in the cover letter for the final ASAC report on airport access control, we stand ready to provide additional assistance to TSA on the issue of airport access control security and employee screening. In particular, it is important that TSA work with the ASAC and industry on the implementation of the recommendations. Some recommendations, like the review of the list of disqualifying criminal offenses, need additional study and review which the ASAC working group could not do in the limited 90-day time frame. Other recommendations, like the use of the FBI RapBack program for recurrent criminal history record checks, require industry input to accelerate current TSA time lines for implementation. At a minimum, it would be prudent for ASAC to produce a follow-up report in a year's time to assess implementation of the recommendations as well as a review of the adequacy of airport access control security measures after such implementation of the recommendations.